

NOMACHINE	NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis	N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell	Last modified: 2019-05-24	Amended: A



NoMachine Enterprise Desktop - Installation and Configuration Guide

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

Table of Contents

Introduction

1. NoMachine Enterprise Desktop - Installation and Configuration Guide

[1.1. About This Guide](#)

How to set-up the Enterprise Desktop

2. Install the Enterprise Desktop

[2.1. Prerequisites](#)

[2.2. Windows Installations](#)

[2.3. Mac Installations](#)

[2.4. Linux Installations](#)

[2.5. RPM Packages](#)

[2.6. DEB Packages](#)

[2.7. TAR.GZ Packages](#)

[2.8. Activating the License \(for Customers\)](#)

Connect to the Enterprise Desktop

3. Initiating a NoMachine Connection (end-user's side)

[3.1. Connecting by Browsers Via Enterprise Desktop Web Tools](#)

[3.2. Connecting by NoMachine Client](#)

[3.3. Preventing Users from Storing Credentials](#)

Configurations and Optimizations

4. Configuring NoMachine Enterprise Desktop

[4.1. Configuring Web Sessions](#)

[4.2. Managing Enterprise Desktop Web Services](#)

[4.3. Using an Alternative Apache Web Server](#)

[4.4. Web Optimizations: Using WebRTC \(Real-Time Web Communication\)](#)

5. Compression Techniques and Optimizations

[5.1. Video Streaming Encoding in Web Sessions](#)

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

[5.2. Video Streaming Encoding in Client Sessions](#)

Enterprise Desktop's Administration

[6. Enterprise Desktop's Configuration](#)

[6.1. Configuration Files](#)

[7. Services Management](#)

[7.1. Accepting Connections](#)

[7.2. Stopping and Starting Enterprise Desktop and Services](#)

[7.3. Stopping and Starting Network Services](#)

[7.4. Local and Network Ports](#)

[7.5. Hiding the NoMachine Monitor and Notification Messages](#)

[7.6. Hiding the Whiteboard and Chat Tools](#)

[7.7. Handling with Discovering of this Server on LAN](#)

[8. Notifications to Users](#)

[8.1. Whiteboard and Custom Notifications](#)

[9. Supported Connection Protocols and Authentication Methods](#)

[9.1. Defining Protocol in Server Configuration](#)

[9.2. Locking Down the Accepted Authentication Methods](#)

[9.3. Changing Port for the NX Protocol](#)

[9.4. Changing Port for the SSH Protocol](#)

[9.5. Connecting to a Server Behind a Firewall \(UPnP Port Mapping\)](#)

[9.6. Using NoMachine DBs for Managing User Access](#)

[10. Users Management](#)

[10.1. Managing Users on the Enterprise Desktop Host](#)

[10.2. Connecting with a Privileged System Account](#)

[10.3. Connecting as a NoMachine Trusted User](#)

[10.4. Guest Users](#)

[11. Sessions' Management](#)

[11.1. Monitoring Sessions](#)

[11.2. Managing Sessions](#)

[11.3. Executing Custom Scripts on Server/Node Events](#)

[12. Connections to the Remote Desktop and Collaborative Sessions](#)

[12.1. Blanking the Remote Screen and Auto Lock Upon Disconnecting](#)

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

[12.2. Configuring Interaction Level to the Physical Desktop](#)

[12.3. Configuring Users and Authorization for Connecting to a Physical Desktop](#)

[12.4. Configuring User's Ability to Disable Accepting Connections](#)

13. Device Sharing, Copy&Paste and File Transfer

[13.1. Connecting Devices](#)

[13.2. Disks](#)

[13.3. Printers](#)

[13.4. USB Devices](#)

[13.5. Network Ports](#)

[13.6. Smartcard Readers](#)

[13.7. Copy and Paste Operations](#)

[13.8. Transferring Files](#)

14. Multimedia and Session Recording

[14.1. Supporting Audio and Microphone](#)

[14.2. Recording your Screen](#)

15. Automatic Updates

16. Logging Facilities

[16.1. Using the System Logging Facilities](#)

[16.2. Redirecting Logs to a Custom File](#)

[16.3. Configuring the Automatic Clean-up of Session Directories](#)

[16.4. NoMachine Log Rotation](#)

Federating the Enterprise Desktop Under a Cloud Server

17. Setting-up a Centralized Access to Multiple Enterprise Desktop Servers

[17.1. Federating the Enterprise Desktop Under a Cloud Server](#)

Introduction

1. NoMachine Enterprise Desktop Installation and Configuration Guide

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

Welcome to the NoMachine Enterprise Desktop - Installation and Configuration Guide v. 6.

What is NoMachine Enterprise Desktop for?

NoMachine Enterprise Desktop is a standalone server that provides unlimited concurrent accesses to the physical desktop of its host. Designed for work sharing sessions and real-time collaboration, remote teaching or assistance, it can be configured for full interaction with the desktop or view-only mode.

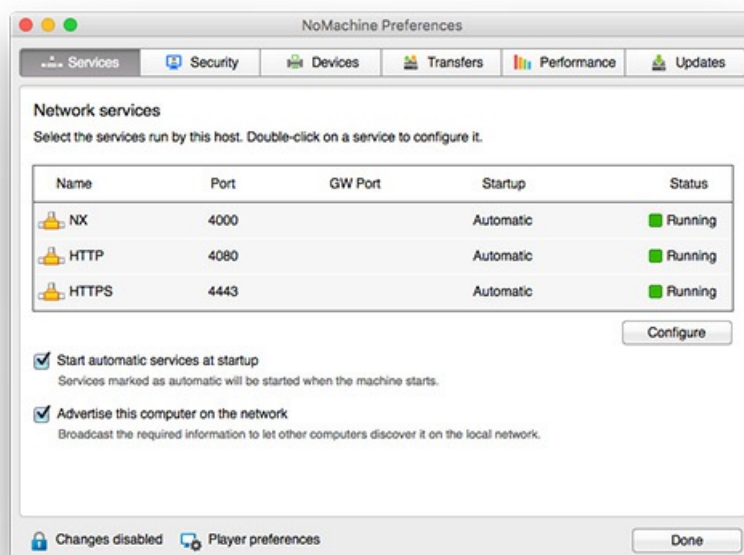
Available for Linux, Mac and Windows, the Enterprise Desktop accepts connections via a browser (thanks to its built-in web server) or via NoMachine client.

Additionally, it can also be federated under a Cloud Server. This solution is suitable to centralize the access to multiple NoMachine servers distributed across the world.

A Graphical Interface

The NoMachine Enterprise Desktop server package includes the NoMachine GUI which provides the graphical interface (Server preferences) for administering the server and its services. This GUI acts also as client for running sessions and connecting to remote desktops.

Most common operations detailed in this guide can be performed by the NoMachine UI and the Server preferences panel running on the local installation of the server:



The server is fully operative once installed

Installation is conceived to provide a fully operative NoMachine server with a default configuration suitable for the greatest part of environments. All the necessary services are automatically started.

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

A standalone server

NoMachine Enterprise Desktop, available for Linux, Windows and Mac, supports multiple concurrent connections to the physical desktop (sharing of the desktop) of its host machine. Number of users is not limited. NoMachine Enterprise Desktop is a single server (standalone server), to all effects.

A federated server

NoMachine Enterprise Desktop can be also federated under a Cloud Server v. 6 which provides a single point of access to multiple server subsystems. In this case, it's possible configuring the Enterprise Desktop to not accept direct connections. For more specific instructions about federating the Enterprise Desktop, refer to the Cloud Server administrative's guide.

1.1. About This Guide

Document Conventions and Important Notices

The following conventions are used in this guide:

BaseDirectory

is the base directory where the NoMachine binaries and libraries are installed.

By default, BaseDirectory is: /usr on Linux, C:\Program Files\ on Windows and /Applications on Mac.

InstallationDirectory

is: *BaseDirectory/NX* on Linux, *BaseDirectory/NoMachine* on Windows and *BaseDirectory/NoMachine.app* on Mac.

The command line interface

NoMachine server and node programs have a command line interface to execute operations.

You need to be a privileged system user to access all these functionalities. These commands can be run from an xterm or similar on Linux and Mac using the sudo utility or as root. On Windows they can be run from a command prompt (cmd.exe) executed as administrator.

On Linux and Mac, invoke the 'nxserver' and 'nxnode' programs from /etc/NX, for example:

```
$ /etc/NX/nxserver --help
$ /etc/NX/nxnode --help
```

on Windows:

move to the 'NoMachine' installation directory, by default it's under C:\'Program files (x86)' on 64bit systems and 'C:\Program file' on 32bits machines and go to the 'bin' subdirectory.

```
> cd C:\PROGRA~1
> cd NoMachine\bin
```

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

```
> nxserver --help
> nxnode --help
```

E.g.:

```
> cd C:\PROGRA~1
C:\Program Files (x86)> cd NoMachine\bin
C:\Program Files (x86)\NoMachine\bin>nxserver --help
C:\Program Files (x86)\NoMachine\bin>nxnode --help
```

The 'nxserver --help' and 'nxnode --help' display the list of all the available commands and options and their description.

Online Resources

Visit the NoMachine Support Area to access a variety of online resources included the NoMachine Forums, tutorials and FAQs: <https://www.nomachine.com/support>

Find a list of all documents and tutorials: <https://www.nomachine.com/all-documents>

Use the Knowledge Base search engine to access articles, FAQs and self-help information: <https://www.nomachine.com/knowledge-base>

Leave Feedback About This Guide

Our goal is to provide comprehensive and clear documentation for all NoMachine products. If you would like to send us your comments and suggestions, you can use the contact tool available at <https://www.nomachine.com/contact-request>, selecting Web Quality Feedback as your option.

2. Install the Enterprise Desktop

2.1. Install the Enterprise Desktop

Supported Operating Systems

Windows 32-bit/64-bit XP/Vista/7/8/8.1/10

Windows Server 2008/2012/2016

Mac OS X Intel 64-bit 10.7 to 10.14

Linux 32-bit and 64-bit

RHEL 4 to RHEL 8
SLED 10 to SLED 15
SLES 10 to SLES 15

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

openSUSE 10.x to openSUSE 15.x
Mandriva 2009 to Mandriva 2011
Fedora 10 to Fedora 30
Debian 4.0 to Debian 9
Ubuntu 8.04 to Ubuntu 19.04

Raspberry Pi 2/3 ARMv6/ARMv7/ARMv8

Hardware requirements

Intel Core2 Duo or AMD Athlon Dual-Core or equivalent
1 GB RAM
Network connection (either a LAN, or Internet link: broadband, cable, DSL, etc...)
Size required on disk:
Windows 210 MB
Linux 195 MB
Mac 180 MB
ARMv6 175 MB
ARMv7 165 MB
ARMv8 185 MB

Software requirements

A desktop environment must already be installed. This applies also to headless Linux machines. Connections by the web and by NoMachine clients are supported.

Compatibility with older versions

Even if it's advisable to upgrade client installations to the same version 6 of the Enterprise Desktop, compatibility with clients v. 4 and 5 is preserved. NoMachine v. 6 is not compatible with the legacy NX version 3.5.0 (no longer supported since December 2016). Note also that when the Enterprise Desktop works as a federated server, NoMachine Cloud Server v. 6 requires a client v. 6.

2.2. Windows Installations

INSTALL

Download the package for Windows from the NoMachine web site and install it by double-clicking on the icon of the executable: a setup wizard will take you through the installation. Accept to reboot the machine, this is mandatory for completing the installation.

If you own a **customer license** we recommend to download the package from your **Customer Area**: <https://www.nomachine.com/support#login>.

TIP



To install the package in **silent** or **very silent mode** from a CMD console, run respectively:

```
>nomachine-packageName_packageVersion.exe /silent
```

or:

```
>nomachine-packageName_packageVersion.exe /verysilent
```


NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

Then reboot the machine:

```
>SHUTDOWN -r -t 10 -c " your comments here"
```

To specify a non-default installation directory, use:

```
>nomachine-packageName_packageVersion.exe /SILENT /DIR="X:Target_directory"
```

or:

```
>nomachine-packageName_packageVersion.exe /VERYSILENT /DIR="X:Target_directory"
```

Note for Windows XP: the NoMachine server will not start until the machine is rebooted.

UPDATE

The update procedure for server and node installations requires to stop all NoMachine services in order to correctly replace libraries and binaries. This implies that the Enterprise Desktop is not accessible to users during the update procedure. Current sessions will be terminated, users will be able to connect again later.

There are two ways to update your current installation:

I Automatic updates

You can update your installation from our repositories. Just run the NoMachine GUI from your Programs Menu and access the 'Settings' panel and click on 'Server preferences'. Go to the 'Updates' GUI and click on the 'Check now' button.

NoMachine has the automatic check for updates enabled: it will check by default our repositories every two days to verify if updates are available. In this case, the server will prompt a dialog informing that a new version is available but **it will never automatically update the current installation.**

Checking for updates can be disabled from that dialog by selecting the 'Don't ask again for this version' option or in the Updates panel by unchecking the 'Automatically check for updates' option.

You can find detailed instructions for configuring the Automatic Updates in a separate document available at: <https://www.nomachine.com/all-documents> .

Note: Due to heavy changes between versions 5 and 6, the automatic updates are disabled: it's therefore necessary to upgrade NoMachine Enterprise Desktop v. 5 by using packages.

II Update with NoMachine packages

Alternatively, download the latest available package from the NoMachine web site and click on the executable file to launch Setup. As for the installation, Setup will guide you through all steps necessary for updating your installation.

If you own a **customer license** we recommend to download the package from your Customer Area: <https://www.nomachine.com/support#login>.

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

UNINSTALL

You can uninstall NoMachine Enterprise Desktop from the Windows Control Panel and the 'Add or Remove Programs' in Windows XP or 'Program and Features' in Windows Vista, 7, 8 or 10. Find the NoMachine program in the list of installed programs and choose to uninstall it.

On Windows 8 or later you can use the Search box from the Charms bar on the right side of the screen: type Control Panel to open it. Then access the Programs - 'Uninstall a program' panel.

On Windows 7, Vista and XP, click on the Start button and click to open the Control panel from the Start menu. Then access panel 'Programs and Features' or 'Add or Remove Programs', depending on your Windows version.

Reboot is requested to complete the uninstalling process.

TIP



To **uninstall from a CMD console**, move to C:/ProgramData/NoMachine/var/uninstall/ (if you are on Vista/7/8/10) or to C:/Documents and Settings/All Users/NoMachine/var/uninstall/ (if you are on XP). Then run:

```
> unins000.exe /silent
```

or:

```
> unins000.exe /verysilent
```

Uninstalling is completed when your command prompt is back. Then, your computer will restart automatically.

2.3. Mac Installations

INSTALL

Download the DMG package from the NoMachine web site. Double-click on the disk Image to open it and see the package icon. Then double-click on the package icon to install the program: the installer will take you through the installation.

If you own a **customer license** we recommend to download the package from your Customer Area: <https://www.nomachine.com/support#login>.

TIP



To install from the command line, run:

```
$ NXMOUNTDIR=$(echo `hdiutil mount nomachine-enterprise-desktop_version.dmg | tail -1 | awk '{\$1=\$2=""}`  
print $0}` | xargs -0 echo)
```

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

```
$ sudo installer -pkg "${NXMOUNTDIR}/NoMachine.pkg" -target /
```

UPDATE

The update procedure for server and node installations requires to stop all NoMachine services in order to correctly replace libraries and binaries. This implies that the Enterprise Desktop is not accessible to users during the update procedure. Current sessions will be terminated, users will be able to connect again later.

There are two ways to update your current installation:

I Automatic updates

You can update your installation from our repositories. Just run the NoMachine GUI from your Programs Menu and access the 'Settings' panel and click on 'Server preferences'. Go to the 'Updates' GUI and click on the 'Check now' button.

NoMachine has the automatic check for updates enabled: it will check by default our repositories every two days to verify if updates are available. In this case, the server will prompt a dialog informing that a new version is available but **it will never automatically update the current installation**.

Checking for updates can be disabled from that dialog by selecting the 'Don't ask again for this version' option or in the Updates panel by unchecking the 'Automatically check for updates' option.

You can find detailed instructions for configuring the Automatic Updates in a separate document available at: <https://www.nomachine.com/all-documents>.

Note: Due to heavy changes between versions 5 and 6, the automatic updates are disabled: it's therefore necessary to upgrade NoMachine Enterprise Desktop v. 5 by using packages.

II Update with NoMachine packages

Alternatively, download the latest available package from the NoMachine web site and click on the executable file to launch Setup. As for the installation, Setup will guide you through all steps necessary for updating your installation.

If you own a **customer license** we recommend to download the package from your Customer Area: <https://www.nomachine.com/support#login>.

UNINSTALL

To uninstall the Enterprise Desktop drag and drop NoMachine from Applications to trash or select 'Move to trash' from the mouse button menu. This will uninstall all the NoMachine software.

TIP



To **uninstall from command line**, it's enough you remove the NoMachine application directory:

```
$ sudo rm -rf /Applications/NoMachine.app
```

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

2.4. Linux Installations

Installing for the first time

You can install, update and uninstall using the graphical package manager of your Linux distribution or from command line by running commands from an xterm or similar with the sudo utility, or as root user if you don't have sudo installed. Instructions below refer to installation by command line.

If you own a **customer license** we recommend to download the package from your Customer Area: <https://www.nomachine.com/support#login>.

Successive updates

The update procedure for server and node installations requires to stop all NoMachine services in order to correctly replace libraries and binaries. This implies that the Enterprise Desktop is not accessible to users during the update procedure. Current sessions will be terminated, users will be able to connect again later.

There are two ways to update your current installation:

I Automatic updates

You can update your installation from our repositories. Just run the NoMachine GUI from your Programs Menu and access the 'Settings' panel and click on 'Server preferences'. Go to the 'Updates' GUI and click on the 'Check now' button.

NoMachine has the automatic check for updates enabled: it will check by default our repositories every two days to verify if updates are available. In this case, the server will prompt a dialog informing that a new version is available but **it will never automatically update the current installation**.

Checking for updates can be disabled from that dialog by selecting the 'Don't ask again for this version' option or in the Updates panel by unchecking the 'Automatically check for updates' option.

You can find detailed instructions for configuring the Automatic Updates in a separate document available at: <https://www.nomachine.com/all-documents>.

Note: Due to heavy changes between versions 5 and 6, the automatic updates are disabled: it's therefore necessary to upgrade NoMachine Enterprise Desktop v. 5 by using packages.

II Update with NoMachine packages

Alternatively, download the latest available package from the NoMachine web site and click on the executable file to launch Setup. As for the installation, Setup will guide you through all steps necessary for updating your installation.

If you own a **customer license** we recommend to download the package from your Customer Area: <https://www.nomachine.com/support#login>.

2.5. RPM Packages

If you want to **install to default location**, namely /usr/NX/:

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

INSTALL

```
# rpm -ivh <pkgName>_<pkgVersion>_<arch>.rpm
```

To find out which NoMachine package you have installed (you will get the full name of the package), run:

```
# rpm -qa | grep nomachine
```

UPDATE

```
# rpm -Uvh <pkgName>_<pkgVersion>_<arch>.rpm
```

UNINSTALL

```
# rpm -e nomachine-enterprise-desktop
```

TIP



For **non-default locations**, for example /opt/NX:

INSTALL

```
# rpm -ivh <pkgName>_<pkgVersion>_<arch>.rpm --prefix /opt
```

UPDATE

```
# rpm -Uvh <pkgName>_<pkgVersion>_<arch>.rpm --prefix /opt
```

UNINSTALL

```
# rpm -e nomachine-enterprise-desktop
```

2.6. DEB Packages

If you want to **install to default location**, namely /usr/NX/:

INSTALL

```
$ sudo dpkg -i <pkgName>_<pkgVersion>_<arch>.deb
```

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

To find out which NoMachine package you have installed (you will get the full name of the package), run:

```
$ dpkg -l | grep nomachine
```

UPDATE

```
$ sudo dpkg -i <pkgName>_<pkgVersion>_<arch>.deb
```

UNINSTALL

```
$ sudo dpkg -r nomachine-enterprise-desktop
```

TIP



For **non-default locations**, for example /opt/NX:

INSTALL

```
$ sudo NX_INSTALL_PREFIX=/opt dpkg -i <pkgName>_<pkgVersion>_<arch>.deb
```

UPDATE

```
$ sudo NX_INSTALL_PREFIX=/opt dpkg -i <pkgName>_<pkgVersion>_<arch>.deb
```

UNINSTALL

```
$ sudo dpkg -r nomachine-enterprise-desktop
```

2.7. TAR.GZ Packages

If you want to **install to default location**, namely /usr/NX/, ensure that package is placed there.

INSTALL

```
$ cd /usr
$ sudo tar xvzf <pkgName>_<pkgVersion>_<arch>.tar.gz
$ sudo /usr/NX/nxserver --install
```

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

UPDATE

```
$ cd /usr
$ sudo tar xvzf <pkgName>_<pkgVersion>_<arch>.tar.gz
$ sudo /usr/NX/nxserver --update
```

UNINSTALL

```
$ sudo /usr/NX/scripts/setup/nxserver --uninstall
$ sudo rm -rf /usr/NX
```

TIP



For **non-default locations**, for example /opt/NX:

INSTALL

```
$ sudo NX_INSTALL_PREFIX=/opt /usr/NX/nxserver --install
```

UPDATE

```
$ sudo NX_INSTALL_PREFIX=/opt /usr/NX/nxserver --update
```

UNINSTALL

```
$ sudo /opt/NX/scripts/setup/nxserver --uninstall
$ sudo rm -rf /opt/NX
```

2.8. Activating the License (for Customers)

Customers' packages

include a temporary (30-days) node.lic and server.lic files for evaluation.

Such license files have to be replaced with the customer's license files acquired from NoMachine. This can be done via the NoMachine server GUI in the 'Updates' panel: click on the server.lic and node.lic links to open their license panel and replace the license.

See <https://www.nomachine.com/DT10000155> for more details on the GUI usage, or

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

<https://www.nomachine.com/AR11O00942> for more instructions, included commands from a terminal to activate licenses manually.

To verify from command line that server.lic and node.lic are correctly in place and check their validity, you may run the nxserver/nxnode --subscription and --version commands. For example on Linux:

```
$ sudo /etc/NX/nxserver --subscription
$ sudo /etc/NX/nxnode --subscription
$ sudo /etc/NX/nxserver --version
$ sudo /etc/NX/nxnode --version
```

3. Initiating a NoMachine Connection (end-user's side)

First of all, ensure that the user has a system account on the Enterprise Desktop host: you can create it by using system tools or by using nxserver commands. Empty password is not supported.

3.1. Connecting by Browsers Via Enterprise Desktop Web Tools

Once installation is complete, Enterprise Desktop is ready to go.

The end-user should point the browser on his/her device to:

<http://SERVER:4080>

Where SERVER is either the name or IP address of the host you want to reach.


E.g., if Enterprise Desktop is installed on a host named 'myserver.com', the URL will look like this:

<http://myserver.com:4080>

Connection will be automatically switched to HTTPS protocol:

<https://myserver.com:4443/nxwebplayer>

In the login form, the end-user has to provide username and password of his/her system account on the Enterprise Desktop host and connect.

TIPS 

I Auto-reconnection is supported: when the connection is lost for whatever reason (including

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

when browser's computer has entered sleep mode), the NoMachine web application will automatically try to reconnect for as long as the user keeps the web page open. If reconnecting is not possible, then the user will have to reconnect manually.

- II IPv6 is supported: specify the IP address of the server host in IPv6 format (e.g. 2001:0:5ef5:79fb:30c6:1516:3ca1:5695) if you want to use it instead of IPv4.

3.2. Connecting by NoMachine Client

From a client device, where you have already installed a NoMachine package type or the Enterprise Client, run the NoMachine GUI from the programs or applications menu. A wizard will take you through the steps necessary to set-up your first connection, just click on 'Create a new connection'. If you prefer to skip the wizard, click on 'Continue'.

The fastest way to create a new connection is to write the name or IP of the NoMachine host you want to connect to in the text field and click on the 'Press enter to create a new connection' link. This method will use the default NX protocol on port 4000.

Alternatively, you can click on the 'New' icon next to the white text field to configure the session in more detail.

TIPS

- I Auto-reconnection is supported: when the connection is lost for whatever reason (including when the client host has entered sleep mode), the client will automatically try to reconnect for as long as the user keeps the GUI open. If reconnecting is not possible, then the user will have to reconnect manually.
- II IPv6 is supported: specify the IP address of the server host in IPv6 format (e.g. 2001:0:5ef5:79fb:30c6:1516:3ca1:5695) if you want to use it instead of IPv4.

See also the NoMachine Enterprise Client - Installation and Configuration Guide available at: <https://www.nomachine.com/all-documents>

3.3. Preventing Users from Storing their Credentials

To prevent NoMachine users from storing their credentials, use the [EnableCredentialsStoring](#) key in the server configuration file. The accepted values are:

player Only users connected via NoMachine client are enabled to save username and password in the connection file stored on their devices (computer, tablet etc ...)

webplayer Only users connected via browser can choose to save their access credentials. They are stored in the browser's cookie, given that the user's browser has cookies enabled.

both All users, regardless if connected via NoMachine client or via web, can store their credentials.

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

none Users cannot save their username and password. They will be requested to provide their log-in credentials at each connection.

For example, to allow only users connecting via NoMachine client to store credentials, set in the server configuration file:

[EnableCredentialsStoring player](#)

4. Configuring NoMachine Enterprise Desktop

4.1. Configuring Web Sessions

The configuration file for the web player program (which provides the graphical front-end) and the web client program (which manages web sessions) is `server.cfg`, located in the `BaseDirectory/NX/etc` on Linux, `BaseDirectory/NoMachine/etc` on Windows and `/Applications/NoMachine.app/Contents/Frameworks/etc` on Mac.

For example on Linux: `/usr/NX/etc/server.cfg`.

Default settings

The `Section` directive defines settings for the NoMachine server(s) where the web player application will connect. This directive, by default, points to localhost and looks like:

`Section "Server"`

`Name "Connection to localhost"`

`Host localhost`

`Protocol NX`

`Port 4000`

`Authentication password`

`EndSection`

Name is a label that can be displayed as an alternative to show hostname of the server.

Host is IP or hostname of the NoMachine server host.

Protocol and **Port** indicates protocol and port that web player will use to connect to the NoMachine server.

Authentication defines the authentication method to be used when connecting by the web: 'password' for password-based authentication (default) or 'private-key' for key-based authentication.

Changing protocol and port

By default when users connect via web, they will use the NX protocol on port 4000. Supported protocols are NX and SSH with system login

To use the NX protocol (this is the default), set:

`Protocol NX`

`Port 4000`

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

To use SSH protocol and system login, set for Linux and Mac:

[Protocol system](#)
[Port 22](#)

and for Windows:

[Protocol system](#)
[Port 4022](#)

Define the authentication method

When connecting by the web and since v. 6.6.8, it's possible to use password-based authentication or key-based authentication (available at the moment only for the NX protocol).

To use password-based authentication (this is the default), set:

[Authentication password](#)

To use SSH key-based authentication, set:

[Protocol NX](#)
[Authentication private-key](#)

TIP



NoMachine uses by default port 22 for SSH protocol on Linux and Mac, and port 4022 on Windows. The default port for NX protocol is 4000. In order to change the port for NX protocol, change the port for the nxd service and restart it. See the paragraph '**Connecting by NX Protocol**'. To change the port for connections by SSH to Linux and Mac hosts it's necessary to modify the listen port for the SSH server on the system. On Windows instead, change the port for the nxsshd service.

Showing hostname or a custom label

To display hostname or IP of the Enterprise Desktop host when connecting by the web, set the following key. This is the default:

[EnableWebConnectionName 0](#)

To display the label set in the 'Name' field of Section "Server" set:

[EnableWebConnectionName 1](#)

Hiding the tutorial wizard at web session startup

To not display the tutorial wizard for the menu panel at session startup, set:

[EnableWebMenuTutorial 0](#)

and to show it (this is the default):

[EnableWebMenuTutorial 1](#)

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

Allowing to log-in as a guest

If the Enterprise Desktop has support for guest users enabled, set the following key if you need that users connect by the web always as guest users:

[EnableWebGuest 1](#)

If this key is disabled, users will have the possibility to choose if log-in with their credentials or as a guest.

4.2. Managing Enterprise Desktop Web Services

You can start and stop the NoMachine HTTP server (nxhtd) from the Server preferences GUI -> Server preferences -> Network services panel. From the NoMachine GUI you can also change the port where the web server will be listening (by default 4080 and 4443 for secure connections).

From command line instead it's possible to do the following.

Stop, start or restart nxhtd

```
nxserver --stop nxhtd

or:

nxserver --start nxhtd

or:

nxserver --restart nxhtd
```

Automatic restart of the nxhtd service

Each service is automatically restarted at the next boot. You can change the default behavior for the nxhtd service by setting:

```
nxserver --startmode nxhtd manual

or to enable the automatic restart of the service:

nxserver --startmode nxhtd automatic
```

The nxserver --startmode command operates on the StartHTTPDaemon server configuration key:

[StartHTTPDaemon Automatic](#)

and:

[StartHTTPDaemon Manual](#)

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

Disabling connections by the web

Edit the server configuration file and remove HTTP from the ClientConnectionMethods key. It should then look like:

`ClientConnectionMethods NX,SSH`

Then restart NoMachine server to make this change effective:

```
nxserver --restart
```

4.3. Using an Alternative Apache Web Server

NoMachine Enterprise Desktop is designed to provide a fully integrated service to deploy sessions on the web which doesn't require additional software to be installed or manual configuration. The minimal Apache web server, nxhtd, provides the necessary modules and is pre-configured to work with the web player application.

However, it is possible to run the web player application with an alternative Apache web server. This requires the configuration of Apache and the web player.

Instructions are available at: <https://www.nomachine.com/DT03O00128>

4.4. Web Optimizations: Using WebRTC (Real-Time Web Communication)

The implementation of WebRTC support in browser-based remote desktop sessions has initially been released as beta and must be enabled explicitly by the administrator by editing the server.cfg file.

With the help of a STUN/TURN server for negotiating NAT traversal, peer-to-peer WebRTC communication can be established also when the web session has to be run behind a NAT.

STEP 1: Uncomment and set the AcceptedWebMethods key as follows to enable the use of WebRTC:

`AcceptedWebMethods webrtc`

STEP 2: If the node machine where the web session will be started is behind a NAT, you need to uncomment the following section in server.cfg:

Section "STUN"

Host hostname
Port portnumber
User username
Password password

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

EndSection

and provide relevant information to contact a STUN or TURN server. In this last case change Section name to "TURN".

See also: <https://www.nomachine.com/AR07N00892> for further intructions about the configuration and: <https://www.nomachine.com/AR07N00894> for an example about how to set up your own STUN/TURN server and configure the Enterprise Desktop accordingly.

5. Compression Techniques and Optimizations

5.1. Video Stream Encoding in Web Sessions

In case of web sessions, by default, session data are streamed in video frames compressed and decompressed by using the MJPEG lossy algorithm, which is the video-format widely supported by browsers.

Oher video codecs like VP8 and H.264, require a browser which supports WebRTC and HTML5.

NoMachine web sessions use the H.264 video streaming when the following requirements are all met, otherwise VP8 is used. In practice, when WebRTC is enabled, the H.264 or VP8 encoding will be used, otherwise MJPEG will be the codec:

- I WebRTC is enabled.
- II The software or hardware H.264 encoding is supported on the server host. (*)
- III The browser supports WebRTC and the H.264 decoding

(*) *Server packages provide the H.264 libraries necessary to support the SW H.264 encoding.*

HW H.264 encoding is possible when the server host machine has an hardware accelerated video cards (GPU) with any of the supported microarchitectures: Nvidia Kepler microarchitecture onward and Intel Quick Sync processors. Enabling HW acceleration by Quick Sync requires however a manual configuration as explained here: <https://www.nomachine.com/AR09O00938>

Optimizations

Optimizations can be done in two ways: (I) by adjusting display settings in the session or (II) by enabling WebRTC.

I **Adjusting display settings in the web sessions**

To access NoMachine display settings, open the NoMachine menu inside the web session: press ctrl+alt+0 or click on the page peel in the upper right corner of the window to open it. Then click on the 'Display' button and finally on 'Display settings'. From this panel you can do the following.

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

Change the display image quality

Increasing the quality will mean to apply a minor compression ratio, the image will be clearer, but more bandwidth will be used.

Disable network-adaptive display quality

This will anchor the display quality to the fixed value specified in the Display quality slider, making it independent from the current network congestion. This is not recommended when there is a very limited bandwidth.

Disable multi-pass display encoding

This will disable the progressive refinement of the image from the lower quality version of the image during moments of inactivity of the desktop till the target quality set in the Display quality slider. Disabling this refinement will send the image directly with target quality. This is not recommended when there is a very limited bandwidth.

II Enabling WebRTC

NoMachine web sessions use by default the classic web media exchange protocol for the two-way browser/web server communication. WebRTC (Real-Time Web Communication) is also supported and can be enabled as explained in the next paragraph.

Enabling WebRTC allows to use the H.264 video streaming (when possible) or VP8 which optimize users'experience with multimedia applications and contents.

TIP



You may verify which encoding method is in use from the NoMachine menu inside the session: press ctrl+alt+0 or click on the page peel in the upper right corner of the window to open it. Then click on the 'Display' button and finally on 'Display settings'. The codec actually on use is reported at the bottom left of the menu.

5.2. Video Streaming Encoding in Client Sessions

Sessions run by NoMachine client use a combination of video and image encoding based on standard codecs and a number of techniques developed by NoMachine. Frames are encoded into a video stream optimized by means of a compression and decompression algorithm of real-time image and audio data. VP8, H.264 and MJPEG encoding are supported.

In general VP8 and H.264 are suitable for all situations, while MJPEG can be an alternative when the end-user's computer is less powerful and the user is experiencing slow responsiveness.

The display encoder can be changed on the server:

from the GUI

In the GUI in the Server Performance panel.

or in the node configuration file

Enable the use of a specific codec by editing the node configuration file and enabling the following two keys:

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

[EnableDisplayServerVideoCodec 1](#)
[DisplayServerVideoCodec CODEC](#)

where CODEC can be: 'vp8','h264' or 'mjpeg'. For example:
[EnableDisplayServerVideoCodec 1](#)
[DisplayServerVideoCodec mjpeg](#)

6. Enterprise Desktop's Configuration

6.1. Configuration Files

The configuration files for the nxserver and nxweplayer/nxwebclient programs is server.cfg. The configuration file for the nxnode program is node.cfg.

They are placed in the:
BaseDirectory/NX/etc directory on Linux

BaseDirectory/NoMachine/etc directory on Windows

/Applications/NoMachine.app/Contents/Frameworks/etc/ directory on Mac.

For example on Linux:
/usr/NX/etc/server.cfg
/usr/NX/etc/node.cfg

The Default Configuration

NoMachine Enterprise Desktop comes with a default configuration that is sufficient to grant a working setup in the majority of environments. NoMachine administrators can tune their installation at any moment and according to their specific needs by setting the related configuration keys. In some cases this will require to restart all NoMachine services.

Edit the Configuration Files

NoMachine configuration files are text files made up of a number of key-value pairs. All the configuration files can be edited manually by a text editor. For example 'vi' can be used on Linux and Mac, and 'notepad' on Windows. On Windows it can be necessary that you copy the cfg file in a different place, edit it and move it to the etc directory.

Be sure to uncomment the configuration key (i.e., remove the '#' pre-pended to the key) to set a value different from the default.

When a configuration key supports an on/off status, set value to '0' to disable it and to '1' to enable it.

Make Changes to the Default Configuration Effective

Changes will be effective with the next new connection without the need to restart the server if not otherwise specified.

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

7. Services Management

Installation and upgrade procedures take care of configuring and starting all the necessary services to make NoMachine Enterprise Desktop ready to accept connections to its physical desktop. The necessary services are configured to be restarted at each reboot of the host machine.

7.1. Accepting Connections

You can stop and start accepting new connections via:

the GUI

from the Server status GUI click on 'Stop the server' and 'Start the server' respectively: this will prevent users from running new connections

or **from command line**

to disable accepting new connections from the command line, run:

```
nxserver --stop
```

or to enable accepting new connections:

```
nxserver --start
```

7.2. Stopping and Starting Enterprise Desktop and Services

All NoMachine services can be stopped via:

the GUI

all NoMachine services can be stopped by the Server status GUI ('Shutdown the server'). When doing so, you will be asked if services must be started at the next reboot or not. You can restart services also from the Server status GUI ('Start the server').

or **from command line.**

Stopping all the NoMachine services

```
nxserver --shutdown
```

This will completely disable access to the server host machine and terminate all connections already running on that host. By default, all services will be restarted when the machine is booted. To override this behavior, specify the `--startmode` option when stopping the services:

```
nxserver --shutdown --startmode manual
```

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

Starting NoMachine server and services

```
nxserver --startup
```

All services will be restarted at the next reboot. To not start services when the machine is rebooted, specify the start mode while running the --startup command:

```
nxserver --startup --startmode manual
```

Specifying the start mode

It's possible to set the 'start mode' (if services will be started automatically at boot or not) by using:

```
nxserver --startmode manual
```

or:

```
nxserver --startmode automatic
```

Stopping and restarting NoMachine server and services

```
nxserver --restart
```

7.3. Stopping and Starting a Network Service

The NoMachine networks services available for NoMachine Enterprise Desktop are nxd, nxhtd (both installed on all platforms) and nxsshd (installed on Windows only):

Program	Default port	Scope	Available on
nxd	4000	Accept connections by NX protocol	Linux, Windows and Mac
nxhtd	4080 and 4443	Accept connections by HTTP protocol (connections by the web)	Linux, Windows and Mac
nxsshd	4022	Accept connections by SSH protocol	Windows

You can stop a single service:

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

via the GUI

in the Server status -> Server preferences -> Network services GUI. You can choose there also the start mode: if the service must be started automatically at the next boot or not.

or **from command line**.

Stopping a service

```
nxserver --stop SERVICE
```

where SERVICE can be:

nxd, the Network Server for accepting connection by NX protocol

nxhtd, the NoMachine web server for web sessions

nxsshd, the SSH server for Windows

Starting or restarting a service

```
nxserver --start nxd
```

```
nxserver --start nxhtd
```

```
nxserver --start nxsshd (on Windows only)
```

or:

```
nxserver --restart nxd
```

```
nxserver --restart nxhtd
```

```
nxserver --restart nxsshd (on Windows only)
```

Specifying the start mode

By default each service is automatically restarted at the next boot. You can configure that on a per-service basis by running:

```
nxserver --startmode SERVICE manual
```

or to restore the default behavior:

```
nxserver --startmode SERVICE automatic
```

Commands above operate on the configuration keys listed below. You can change them manually in the server configuration.

Configuration	Key setting
Enable automatic starting of the NX Network server, nxd	StartNXDaemon Automatic

Prepared by:
Silvia Regis

N°:
D-705_003-NMC-NTD

Approved by:
Sarah Dryell

Last modified:
2019-05-24

Amended:
A

Disable automatic starting of the NX Network server, nxd	StartNXDaemon Manual
Enable automatic starting of the NoMachine web server, nxhtd	StartHTTPDaemon Automatic
Disable automatic starting of the NoMachine web server, nxhtd	StartHTTPDaemon Manual
Enable automatic starting of the SSH server, nxsshd on Windows	StartSSHDaemon Automatic
Disable automatic starting of the SSH server, nxsshd on Windows	StartSSHDaemon Manual

7.4. Local and Network Ports

For each session, NoMachine uses ports that are used only locally on the server host and network ports.

Some ports are mandatory and must be free, e.g. the session display number and the connection port. Other ports are used for services that can be disabled (e.g. USB forwarding, UDP communication).

Local port	Description	How to change the default
11000 + DisplayBase	Session display. If this port is already in use, NoMachine will look for a free port by incrementing DisplayBase up to the value set in the DisplayLimit server configuration key.	DisplayBase (by default 1001) and DisplayLimit (200) are defined in server.cfg
20000	Communication port between the session's nxserver process and the main server process.	Add the ServerSlaveBase key to the end of server.cfg and specify a value
24000 + DisplayBase	Session's monitor port.	DisplayBase (by default 1001) and DisplayLimit (200) are defined in server.cfg
5473 and 5483	USB devices forwarding.	Disable USB sharing by setting EnableUSBSharing none in node.cfg

Network port	Description	How to change the default
6000 + DisplayBase	TCP port for the NoMachine display service. If this port is already in use, NoMachine will look for a free port by incrementing DisplayBase up to the value set in the DisplayLimit server configuration key.	DisplayBase (by default 1001) and DisplayLimit (200) are defined in server.cfg
5353	UDP port for the MDNS service to broadcast computer's information over the LAN.	Disable the service by setting EnableNetworkBroadcast 0 in server.cfg
	TCP port for the NoMachine Network	

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

4000	service (nxd) and connections via NX protocol. This port must be open in the firewall and mapped to the external IP of the server host.	Set NXPort in server.cfg and restart the nxd service.
4011 - 4999	UDP port range.	Set UDPPort in server.cfg to define a different range. UDP can be disabled on client side.
22 (Linux and Mac)	TCP port for connections via SSH protocol on Linux and Mac. This port must be open in the firewall and mapped to the external IP of the server host.	Set a different port for the system SSH server and align value set for SSHDPort in server.cfg. Then restart the NoMachine server.
4022 (Windows)	TCP port for the NoMachine SSH server on Windows (nxsshd) and connections by SSH protocol. This port must be open in the firewall and mapped to the external IP of the server host.	Set SSHDPort in server.cfg and restart the nxsshd service.
4080 and 4443	HTTP and HTTPS port for web connections. These ports must be open in the firewall and mapped to the external IP of the server host.	Change 'Listen' directives in htd.cfg and restart the nxhtd service.
20000 - 30000	External ports range for UPnP port mapping.	Set NXUPnPPort in server.cfg to define a different range. Set EnableUPnP none in server.cfg to disable port mapping
5040 + x	Port opened between client and server for each USB device. Port number is defined by 5040 + x where 'x' is the first free port retrieved starting from port number 5040.	N/A
4000	Automatic updates from NoMachine repositories.	Updates are managed by nxd. Disable automatic updates by setting UpdateFrequency 0 in server.cfg
5473 and 5483	USB devices forwarding.	Disable USB sharing by setting EnableUSBSharing none in node.cfg

7.5. Hiding the NoMachine Monitor and Notification Messages

It is possible to hide or show the !M (the Monitor) icon in the system tray. When the icon is hidden, notification messages will still be displayed when users are connecting. This can be configured:

from the GUI:

In the Server status -> Server preferences -> Server options GUI. When the icon is hidden, notification messages will still be displayed when users are connecting.

or in the **node configuration file**

This setting is ruled by the [DisplayMonitorIcon](#) key in the node configuration file. If you change them manually by editing the file, you then need to restart the server to make changes effective.

To hide the !M in the system tray set:

[DisplayMonitorIcon 0](#)

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

To display the !M in the system tray set:

[DisplayMonitorIcon 1](#)

In both cases, then restart the server:

```
nxserver --restart
```

By default NoMachine issues a ballon message to notify about events like user's disconnection or user's requests for connecting. You can disable notification messages by setting the following key in the node configuration:

[DisplayMonitorNotifications 0](#)

TIP



If the displaying of monitor's notification messages is disabled, the desktop owner will be unable to accept connection's requests by other users. Configure trusted users if you need to permit the connection without explicit authorization.

7.6. Hiding the Whiteboard and Chat Tools

If you want to disable the possibility of launching the Whiteboard from the Monitor menu, edit the node configuration file to have:

[EnableWhiteboard 0](#)

Then restart the server:

```
nxserver --restart
```

7.7. Handling with Discovering of this Server on LAN

By default NoMachine Enterprise Desktop broadcasts information to let other NoMachine computers to discover it on the local network. You can disable this feature via:

the GUI

in the Server status -> Server preferences -> "Network services" GUI

or in **the server configuration file**

set the following key in the server configuration:

[EnableNetworkBroadcast 0](#)

Then restart the server to make changes effective:

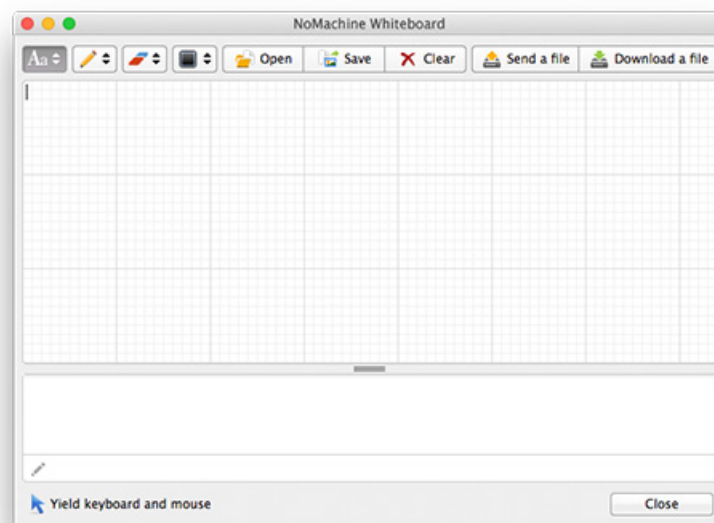
NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

```
nxserver --restart
```

8. Notifications to Users

8.1. Whiteboard and Custom Notifications

NoMachine provides an instant messaging tool, named **whiteboard** which allows also drawing and sharing files with connected users and fast-track access to file transfer. To access it, connect to the user's desktop and from the Monitor (!M icon) in your system tray click on 'Show the whiteboard'. Note that if multiple users are connected at the same time, they will all see the message.



As an alternative, it's possible to issue a dialog in the connected sessions to show a custom message by sending it from command line.

Sending a message to all running sessions:

```
nxserver --broadcast "Your message goes here"
```

or sending a message only to the session specified by its session id:

```
nxserver --message "Your message goes here"
```

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

9. Supported Connection Protocols and Authentication Methods

NX Protocol

connections by default use the NX protocol which is its own protocol for secure communication over the network. Encryption in the NX protocol is implemented using OpenSSL TLS/SSL, based on ECDHE-RSA-AES128-GCM-SHA256 as the default cipher suite. ECDHE-RSA-AES128-GCM-SHA256 is an AES (Advanced Encryption Standard) block cipher with 128 bits key in GCM (Galois/Counter Mode). RC4 (ECDHE-RSA-RC4-SHA cipher suite) is used as a backward compatibility when connecting from or to versions 4.0.

When using the NX protocol, NX data can travel on TCP and UDP streams, even at the same time. The client and server can decide dynamically what transport to use, based on the type of data and the network conditions. Client and server negotiate the UDP transport at session startup, after having negotiated the main TCP link. UDP uses symmetric Blowfish encryption, with key negotiated on the secure TCP link. UDP is presently not available when using the SSH tunneling, to ensure that all data goes through the same SSH link, as it was in legacy version 3. UDP protocol can be also disabled.

SSH Protocol

NoMachine Enterprise Desktop also provides tunneling of connections using SSH and full integration with any authentication backend supported by the host SSH server. On Windows systems, NoMachine provides a built-in SSH server, nxsshd.

Authentication methods

These are the authentication methods supported by NoMachine when connections use the NX protocol or the SSH protocol:

Authentication method	NX protocol	SSH protocol
Login with user's password	yes	yes
Login with SSH private key(*)	yes	yes
Login with SSH private key provided by a SSH agent (<i>available since v. 6.3.6</i>)	-	yes
Login with SSH private key stored on a smart card(*)	-	yes
Login with Kerberos ticket on client side(**)	yes	yes
(*)Support for SSH agent forwarding	-	yes
(**)Support for Kerberos tickets authentication forwarding	yes	yes
Support for two-factor authentication	yes	yes

9.1. Defining Protocol in Server Configuration

Protocols are defined in the [ClientConnectionMethods](#) key in the server configuration. They are

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

specified as a comma-separated list of values:

[ClientConnectionMethods NX,SSH,HTTP](#)

This key is automatically populated during the installation or the update of the package. It is possible to exclude any of the available protocols to force users to connect by the desired protocol.

For example, to use only NX protocol, set this key to:

[ClientConnectionMethods NX](#)

and restart the server to make changes effective:

```
nxserver --restart
```

TIPS

- I If your server supports SSH but it still reports that SSH is not available, check the `ClientConnectionMethods` key and ensure that the SSH values is set. Then restart the server.
- II Removing 'HTTP' from the `ClientConnectionMethods` key will disable the starting of the NoMachine HTTP server and prevent connections via web.

9.2. Locking Down the Accepted Authentication Methods

Administrators may decide how the user should authenticate on the server by defining which authentication method(s) is/are available. Authentication methods can be set in the server configuration file by editing this key:

[AcceptedAuthenticationMethods all](#)

By default all methods are accepted. They can be restricted by providing a comma-separated list of values, they will indicate which authentication method is permitted.

Accepted values for **connections by NX protocol** are:

[NX-password](#) to allow password authentication.

[NX-private-key](#) to allow key-based authentication.

[NX-kerberos](#) to allow Kerberos ticket-based authentication.

while for **connections by SSH protocol**:

[SSH-system](#) to allow all methods supported for the system login. SSH authentication methods for the system login have to be set on the system for example in the PAM configuration.

For example, to accept key-based and Kerberos ticket-based authentication for the NX protocol:

[AcceptedAuthenticationMethods NX-private-key, NX-kerberos](#)

Settings in the client GUI

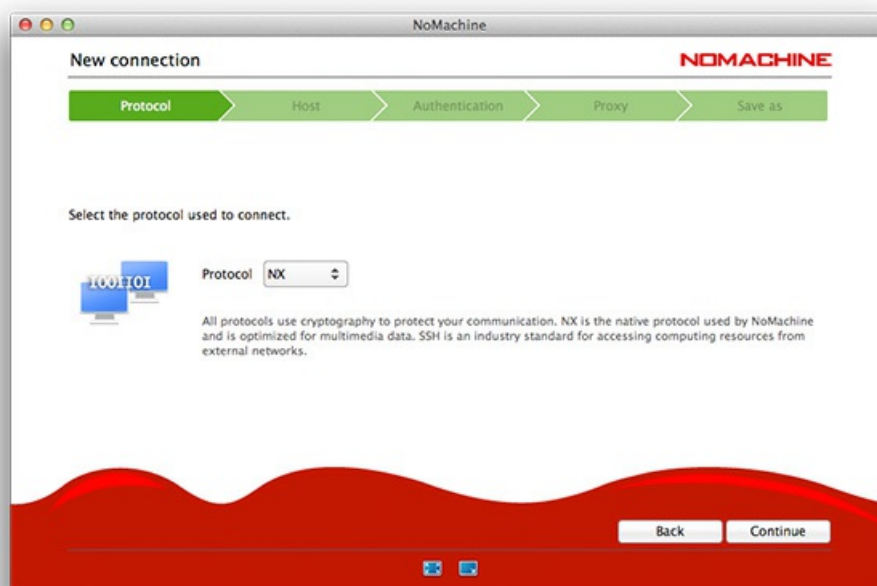
NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

Users can select the authentication method in their connection settings from the NoMachine GUI in the Advanced panel for the NX protocol and SSH protocol settings respectively.

They correspond to the following options in the client GUI:

Authentication method	NX protocol Client GUI's Advanced settings options	SSH protocol Client GUI's Advanced settings options
Login with user's password	Password (default)	Password (default)
Login with SSH private key(*)	Private key	Private key
Login with SSH private key provided by a SSH agent (<i>available since v. 6.3.6</i>)	-	Authentication agent
Login with SSH private key stored on a smart card(*)	-	Smart card
Login with Kerberos ticket on client side(**)	Kerberos	Kerberos
(*)Support for SSH agent forwarding	-	Private key + Forward authentication or Smart card + Forward authentication
(**)Support for Kerberos tickets authentication forwarding	Kerberos + Forward authentication	Kerberos + Forward authentication
Support for two-factor authentication	No settings needed on client side, it's a server side configuration	No settings needed on client side, it's a server side configuration

Protocol and authentication methods can be set when creating a new connection via client GUI:



NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

or changed later by modifying the connection settings (right mouse click on the connection icon in the client GUI to edit it).

9.3. Changing Port for the NX Protocol

The default setting of NoMachine is to run connections via the NX protocol on port 4000. On server side, the Network Server, nxd, is listening on port 4000. It's mandatory that this port is open between client and server to allow connections by NX protocol.

If you change the listen port for nxd, connecting users will have to specify the new value in their connection settings in the client GUI.

It's possible to modify the port for nxd

from the GUI

in the Server status -> Server preferences -> Network services GUI

or in the **server configuration file** by editing this key:

[NXPort 4000](#)

Restarting the nxd service is necessary to make this change effective:

```
nxserver --restart nxd
```

When NX protocol is used, **UDP** communication for multimedia is enabled by default. UDP traffic uses a range of ports between 4011 and 4999. These ports must be open between client and server. If they are not available, traffic will fall back to TCP communication. You can change port range, define a comma-separated list of ports or a single port by changing value set for the following key in the server configuration:

[UDPPort 4011-4999](#)

Users can disable UDP in their connection settings from the NoMachine GUI in the Advanced panel for the NX protocol settings.

9.4. Changing Port for the SSH Protocol

The default port used for the SSH protocol is 22 **on Linux and Mac**. On such platforms NoMachine relies on the SSH server installed on the system. If your SSHD is configured to listen on a port different from 22 you need to align the NoMachine server configuration accordingly. Connecting users will have to specify such value in their connection settings in the client GUI.

If your SSH server is listening on a port different than 22, change the SSH port in the NoMachine configuration

in the Server status -> Server preferences -> Network services GUI

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

or in the **server configuration file** by editing this key:
[SSHDPort 22](#)

On Windows, NoMachine provides the SSH server, nxsshd, listening on port 4022. As explained above, this port can be changed from the GUI or in the server configuration file ([SSHDPort 4022](#)).

Restarting the nxsshd service is necessary to make this change effective:

```
nxserver --restart nxsshd
```

9.5. Connecting to a Server Behind a Firewall (UPnP Port Mapping)

Automatic discover of the NoMachine Enterprise Desktop host is possible only when the server and the user's machine are on the same LAN. When the user connects over the internet or from a different network, it's mandatory to know the public (or external) IP of the Enterprise Desktop.

When the server is behind a firewall, you have to configure the router to forward external port to the nxd service (to use the NX connection protocol), to the SSH server (to use the SSH protocol) and to the nxhtd service (to connect by the web). By default the required ports are TCP ports: 4000 for NX, 4080 and 4443 for HTTP/HTTPS and UDP ports in the 4011-4999 range. Note that users will have to specify the external port in their connection settings in the client GUI.

If the router on the server side supports UPnP/NAT-PMP, you can let NoMachine try to enable port forwarding in the router automatically. External ports will be selected randomly from the 20000 - 30000 range. Also in this case users will have to specify the external port in their connection settings in the client GUI.

For connections by NX protocol, at session startup NoMachine will also try to map UDP ports by using UPnP.

Enabling the automatic port forwarding

Step 1: Set in the server configuration:
[EnableFirewallConfiguration 1](#)

Step 2: Specify for which service the port forwarding must be enabled by listing them in the following key:
[EnableUPnP NX,SSH,HTTP](#)

Step 3: Specify the port where the NX service will be redirected by editing respectively:
[NXUPnPPort ""](#); [SSHUPnPPort ""](#) and [HTTPUPnPPort ""](#)

TIP



To permit only connections by SSH (on external port 20048 for example) and use the automatic port forwarding, set in the server configuration:

[ClientConnectionMethods SSH](#)
[EnableFirewallConfiguration 1](#)
[EnableUPnP SSH](#)
[SSHUPnPPort "20048"](#)
and restart the server.

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

You can enable port forwarding for connections by NX and HTTP/HTTPS protocol also **from the GUI** via the Server preferences -> Network services GUI by selecting the service and enter its settings (click on 'Configure'). Then check the Gateway port option.

Retrieving information about UPnP port mapping

When the automatic port mapping is enabled, you can retrieve information about UPnP port mapping, e.g. IP of the gateway device, external port and port mapped by running:

```

nxserver --upnpstatus

To terminate port mapping:

nxserver --upnpunmap

To initiate port mapping:

nxserver --upnpmap

You can also specify for how long port mapping should last by using

nxserver --upnpmap --time

```

9.6. Using NoMachine DBs for Managing User Access

Use of NoMachine DBs can be configured by editing the server configuration. The table below reports which configuration key value has to be set to enable or disable specific behavior as defined in the 'Target' field:

Target	Server configuration key	Description
User's access based on system authentication (default)	EnablePasswordDB 0	Authentication is requested to the system, user's connection is allowed once the user has been authenticated. PAM, LDAP, AD are supported.
User access based on NX Password db	EnablePasswordDB 1	Authentication is verified against the NX password DB. Separate the NoMachine authentication from the system authentication. The user's account must exist on the system.
Allow connections from all authenticated users (default)	EnableUserDB 0	Every time a new account is created via NoMachine or an already existing system user runs the session for the first time, the user is added to the NoMachine NX Users DB, even when the use of NX Users DB is disabled. These users cannot

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

		be disabled and are always allowed to connect if they authenticate successfully.
Enable or disable user's access to NoMachine	EnableUserDB 1	By default all users are enabled to access the NoMachine system once authenticated. With this configuration a user can be disabled and re-enabled at any moment from command line.

10. Users Management

10.1. Managing Users Enterprise Desktop Host

You can manage (create, delete and modify) user accounts by using tools provided by your Operating System or the NoMachine server commands as explained below.

Creating Accounts

The Enterprise Desktop is able to handle two types of accounts: system accounts and NoMachine accounts. The latter allows to separate the system password from the NoMachine password.

Creating a System Account

The system account will be created with the default system settings. The new user will be also added to the NoMachine Users db:

```
nxserver --useradd USERNAME --system
```

Creating a NoMachine Account

Use this command when the user already has a system account:

```
nxserver --useradd USERNAME
```

TIPS

- I To assign a password different from system password to a system user, enable NoMachine Password DB ([EnablePasswordDB 1](#)) in server.cfg.
- II To verify if the user's authentication is based or not on NoMachine Password db:

```
nxserver --userauth USERNAME
```

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

III If this Enterprise Desktop is federated under a Cloud Server, each user must have the same system account on the Cloud Server host and on this Enterprise Desktop. Password can be different.

Enabling and Disabling access for a NoMachine User

Prerequisites are:

i) The user has run at least one session **or** have been added to NoMachine dbs by means of 'nxserver --useradd' command.

ii) NoMachine Users DB is enabled ([EnableUserDB 1](#) is set in server.cfg)

You can enable/disable a user and allow/forbid his access to the Enterprise Desktop by running:

```
nxserver --userenable USERNAME
```

or:

```
nxserver --userdisable USERNAME
```

Note that 'nxserver --useradd USERNAME' adds the user to NoMachine dbs and automatically enables the user to log-in, while 'nxserver --userdel USERNAME' removes the user from NoMachine dbs and disables the user's ability to login by NoMachine.

Modifying the User's Password

You can modify user's system password by running:

```
nxserver --passwd USERNAME --system
```

or you can modify just the NoMachine password when Password db is in use ([EnablePasswordDB 1](#) is set in server.cfg):

```
nxserver --passwd USERNAME
```

Listing the NoMachine Users

All users who have run at least one session or have been added to NoMachine dbs are stored in the Users db. You can retrieve the complete list by running:

```
nxserver --userlist
```

The output of this command provides the following fields:

Redirected to: IP/hostname of the server to which the user's connection is redirected (by means of the 'nxserver --redirect' command when supported).

Trusted for: it shows if the user is trusted and therefore allowed to connect to the physical desktop of this host (only specific user are permitted to do that).

Screen Sharing: it shows which user has the sharing of their physical screen disabled.

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

Access: it shows if the user is enabled or not to access the NoMachine system. This works in conjunction with the use of the NoMachine Users DB: when enabled ([EnableUserDB 1](#) in the server configuration), it's possible to enable/disable user's access to the whole NoMachine system.

Forwarded to: this field is applicable only when the server is a NoMachine Cloud Server, so it's always empty in case of Enterprise Desktop.

Removing Accounts

To remove an account from the system:

```
nxserver --userdel USERNAME --system
```

or removing a NoMachine user and delete his account from the NoMachine dbs:

```
nxserver --userdel USERNAME
```

This will not remove the system account.

Configuring user's ability to accept or not connections

To switch off/on screen sharing for a given user, use the following server commands. The user, however, will be still able to change it from the !M Monitor menu:

```
nxserver --useredit USERNAME --screensharing yes
```

or:

```
nxserver --useredit USERNAME --screensharing no
```

10.2. Connecting with a Privileged System Account

By default, NoMachine allows the running of sessions as privileged system user ('root' on Linux and Mac and an administrator on Windows). You can however configure the NoMachine Server to disallow it. Do it by disabling the following server configuration key:

[EnableAdministratorLogin 0](#)

To re-enable the possibility to log in as root or administrator, set:

[EnableAdministratorLogin 1](#)

10.3. Connecting as a NoMachine Trusted User

By default when the connecting user is different from the owner of the physical desktop, the desktop

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

owner has to authorize the user for the connection.

It is possible to define in advance a number of trusted users who don't need the specific owner's permission.

In order to create a list of trusted users, administrators should use the nxserver commands for creating and editing users. These commands provide the --trusted option to define if the user is trusted for connections to the physical desktop or not.

To create a new trusted user on the system:

```
nxserver --useradd USERNAME --system --trusted physical
```

For example on Linux and Mac:

```
/etc/NX/nxserver --useradd nctest01 --system --trusted physical
```

To make an existing user trusted, modify trusted permissions or remove them:

```
nxserver --useredit --trusted [physical | none]
```

For example on Linux and Mac, edit user 'nctest02' and give it trusted authorization:

```
/etc/NX/nxserver --useredit nctest02 --trusted physical
```

To remove trusted authorization for user 'nctest01' on Linux or Mac:

```
/etc/NX/nxserver --useredit nctest01 --trusted none
```

To make a user trusted for specific users' desktops

This feature is available since v. 6.4.6. You can assign the 'trusted' flag and make the user trusted only for those desktops owned by a specific user or list of users. For example, if a new user (userB) should be created on the system and made trusted only for desktops of userA:

```
nxserver --useradd userB --system --trusted physical --per-user userA
```

It's also possible to specify more users in a comma-separated list, e.g.:

```
nxserver --useradd userB --system --trusted physical --per-user userA,userC,userD
```

To list only trusted users:

```
nxserver --userlist --trusted
```

10.4. Guest Users

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

The Enterprise supports the possibility to generate guest accounts on demand. The automatic generation of guests accounts is available on all platforms, i.e. Linux, Windows and Mac. This feature however is not enabled by default and must be activated via a profile rule.

Once enabled, the Enterprise Desktop will accept the request to log-in as and automatically create a system account. Time of validity and other features can be set for guest users by editing the server configuration

To enable guest accounts:

```
nxserver --ruleadd --class feature --type enable-guest --value yes
```

To disable login as a guest:

```
nxserver --ruleadd --class feature --type enable-guest --value no
```

TIP



Guest users don't know their username and password and cannot unlock the remote screen if screen locking is enabled. It's therefore necessary to disable it on the system.

Configuring guest accounts

Define range of names for guest accounts

The server creates guest accounts by adding a progressive number as a postfix to the base guest name. The range used for incrementing the postfix varies from a minimum and a maximum value. Base name and range for the postfix are configurable:

```
BaseGuestUserId 10
GuestUserIdLimit 200
```

Define group for guest accounts

```
GuestUserGroup guest
```

Define where the server has to create the guest accounts' homes

```
GuestUserHome /home (e.g. for Linux)
```

Define for how long guest accounts have to be kept before being expired

Default is 30 days:

```
GuestUserAccountExpiry 2592000 (This value has to be set in seconds)
```

Define if guest accounts have to be deleted once expired

```
EnableGuestWipeout 1
```

Setting Disk Quota for Guest Accounts on Linux

The following server configuration keys allow to set disk quota for guest accounts:

```
GuestQuotaProtoname protoguest
GuestQuotaInodeHardlimit 0
GuestQuotaBlockSoftlimit 0
GuestQuotaBlockHardlimit 0
```

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

[GuestQuotaNodeGracePeriod 0](#)
[GuestQuotaBlockGracePeriod 0](#)
[GuestQuotaFilesystems all](#)

Define the maximum number of guests allowed to be created on this server
[GuestUserLimit 10](#)

Define the maximum number of sessions a guest can run on this server before the account expires
[GuestUserConnectionLimit 5](#)

Define for how long (in seconds) a guest can run the session before the account expires
[GuestConnectionExpiry 0](#) (If value is set to 0, a guest's session is never terminated.)

11. Sessions' Management

Each session on the same server is uniquely identified by a **session id** (which can look like: B253864E822F5A235825F3AB8853AF00) and a **display id** (e.g.,1002).

A session on the NoMachine Enterprise Desktop can be in any of the following statuses:

Connected - when it's connected to the remote display.

Finished - the session has been closed in a clean way and all NoMachine processes have been shut-down smoothly.

Failed - Any of the NoMachine processes has failed to start or it has been "un-cleanly" terminated. Transitional statuses are **Connecting** and **Terminating**.

NoMachine Enterprise Desktop is able to manage only connections to the remote physical desktop. You can see the complete list of supported session types by running the following command, which will report 'physical-desktop yes':

```
nxserver --resourcelist --class session
```

11.1. Monitoring Sessions

You can monitor sessions from command line tools. Below are the server commands to be run from xterm or console.

Listing Running Sessions

To list all the running sessions, their display, session owner, remote IP of the connected client, session ID and session host:

```
nxserver --list
```

You can also filter results on a per-user basis:

```
nxserver --list USERNAME
```

NOMACHINE	NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis	N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell	Last modified: 2019-05-24	Amended: A

or gather further information about connected clients:

```
nxserver --list --client-version --client-platform
```

The number of active connections on the server corresponds to the number of sessions in status Connected. Session status is shown in the output of session history command.

Session History

History is preserved for a certain amount of time as set in the server configuration ([SessionHistory](#) key). To see the complete list of sessions, including those that have been cleanly terminated or failed, run:

```
nxserver --history
```

To redirect the output of the session history to a file (available since v. 6.7):

```
nxserver --history --file FILE
```

If you want to filter results on a per-user basis:

```
nxserver --history USERNAME
```

or to get more details about a session:

```
nxserver --history SESSIONID
```

Debugging a Failed Session with Session History

If a session is marked as failed in the session history output, the following command should provide information about the reason of the failure. Since v. 6.7 the output of the following command has been extended to provide a short report helpful for a preliminary debug of the problem:

```
nxserver --history SESSIONID
```

To redirect the error report to a file:

```
nxserver --history SESSIONID --file FILE
```

Retrieving Statistics about Sessions with Session History

This feature is available since v. 6.7. It elaborates a number of information about sessions, contained in the current session history. For example the number of sessions started, terminated, running and failed and their average startup time. The command to retrieve statistics is:

```
nxserver --history --stats
```

To redirect statistics to a file:

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

```
nxserver --history --stats --file FILE
```

Clearing Sessions History

You can reset the history backlog by running the following command.

```
nxserver --history clear
```

Configuring the Session History Backlog

Data is preserved for 30 days. You can modify that in the server configuration file by uncommenting and setting a different value for the following key:

[SessionHistory 2592000](#)

This key accepts the following values:

- < 0 Never delete data from NX session history.
- 0 Disable NX session history.
- > 0 Keep data in session history for this amount of seconds.

11.2. Managing Sessions

Terminating Sessions Automatically

If you need to terminate a remote desktop session after a certain time of inactivity, you can specify it by uncommenting and adding the '-timeout s' (s stays for seconds) option to the DisplayAgentExtraOptions key in the node configuration file.

For example, if you want to terminate sessions after 10 minutes of inactivity you need to set:

[DisplayAgentExtraOptions "-timeout 600"](#)

If the NoMachine display agent doesn't receive any input from the user in the given timeout, it will terminate the session.

Terminating the Session from Command Line

To terminate a remote desktop session you can run:

```
nxserver --terminate SESSIONID
```

or:

```
nxserver --terminate DISPLAYID
```

To terminate all sessions of a certain user, run instead:

```
nxserver --terminate USERNAME
```

If you want to terminate all sessions, just restart the server:

Prepared by:
Silvia Regis

N°:
D-705_003-NMC-NTD

Approved by:
Sarah Dryell

Last modified:
2019-05-24

Amended:
A

```
nxserver --restart
```

If you want to terminate all sessions and forbid new connections until the server is started again:

```
nxserver --shutdown
```

Limit the number of concurrent connections The maximum number of concurrent connections to the physical desktop is defined in the server configuration (twenty by default). Set a different value in this key to increase or decrease the limit:

[ConnectionsLimit 20](#)

11.3. Executing Custom Scripts on Server/Node Events

The **server configuration** provides a number of keys that can be activated to execute a custom script upon a certain event. According to the event, a number of parameters can be specified for each script. In a similar way, a number of keys is present in the **node configuration** file to allow to execute a custom script on a certain NoMachine node event. In both cases and according to the event, a number of parameters can be specified for each script. Keys and parameters not supported by the Enterprise Desktop are omitted in the table below.

Available for	Configuration key	Accepted parameter (server.cfg)	Accepted parameter (node.cfg)
server	UserScriptBeforeLogin	remote ip	-
server	UserScriptAfterLogin	username <i>Starting from v. 6.4, it accepts also</i> remote ip	-
server	UserScriptAfterLogout <i>(available since v. 6.6.8)</i>	username, remote ip	-
server,node	UserScriptBeforeSessionStart	session id, username, node host, node port	session id, username, session type, display
server,node	UserScriptAfterSessionStart	session id, username, node host, node port	session id, username, session type, display
server,node	UserScriptBeforeSessionClose	session id, username, node host, node port	session id, username, session type, display
server,node	UserScriptAfterSessionClose	session id, username, node host, node port	session id, username, session type, display
server	UserScriptBeforeSessionFailure	session id, username, node host, node port	-
server,node	UserScriptAfterSessionFailure	session id, username, node host, node port	session id, username, session type, display
server	UserScriptBeforeCreateUser	username	-
server	UserScriptAfterCreateUser	username	-
server	UserScriptBeforeDeleteUser	username	-

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

server	UserScriptAfterDeleteUser	username	-
server	UserScriptBeforeEnableUser	username	-
server	UserScriptAfterEnableUser	username	-
server	UserScriptBeforeDisableUser	username	-
server	UserScriptAfterDisableUser	username	-

Note that order of parameters is relevant. For example, a custom script to be run on node event 'UserScriptBeforeSessionStart' should use the \$2 variable to retrieve username and \$4 to retrieve display.

A further key in the node configuration file (available since v. 6.3.6), allows to run a custom script triggered on change resolution events (resize of the remote screen). The related key is: [UserScriptAfterRemoteResize](#)

Pre-requisites to run custom scripts

Custom scripts must be executable. Custom scripts set-up in server.cfg are common to all the users who are accessing the server and are executed by the nxserver program. Since nxserver is running as the nx user, you have to grant this user the necessary permissions in order to execute the custom script.

Custom scripts set-up in node.cfg are executed by the nxnode program, which is run as the connected user. Place the script in a directory that is accessible by the node, i.e. accessible by the connected user(s).

By default if the execution of the scripts fails, the nxserver and nxnode will terminate. This means that the user's session will not start. You can override this behavior by forcing exit 0 inside the custom script and let the session start even if the custom script is failed.

TIP



If NoMachine Enterprise Desktop is federated under a Cloud Server consider that custom scripts have to be placed in server.cfg or node.cfg file on the Enterprise Desktop host, not on the Cloud Server.

12. Connections to the Remote Desktop and Collaborative Sessions

By default users can connect to the remote physical desktop of the Enterprise Desktop host. When the desktop owner is different from the connecting user, he/she is always required to authorize the incoming request for connection.

Authorization is not requested when the incoming user and the desktop owner are the same.

Rather than allow all users to connect without desktop's owner authorization or click accept for every

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

single user which would like to connect, it is possible to define in advance a number of **trusted users** who don't need the specific owner's permission.

Request for desktop owner's authorization and interaction level can be configured **from the GUI**

You can configure how users will connect to a desktop owned by another user from the Server status -> Server preferences -> Desktop access GUI. You can basically determine if users can connect or not without asking the desktop owner's permission and if users will be able to interact with the desktop.

or in the **server configuration** as explained in detail in the next paragraphs.

TIPS 💡

- I Disabling the request for desktop owner's authorization before connecting can be useful in case of remote administration of headless machines.
- II Allowing connections in interactive mode grants the user full access to the desktop resources and applications. View-only mode is suggested for example when making presentations or teaching a lesson.
- III When the Enterprise Desktop is federated under a Cloud Server, each user must have the same system account on the Enterprise Desktop host and on the Cloud Server host. Password can be different.

NoMachine Enterprise Desktop supports also the **screen blanking** (the physical monitor is obscured until somebody is connected from remote) and the **automatic lock of the remote screen** when the last NoMachine user disconnects.

12.1. Blanking the Remote Screen and Auto Lock Upon Disconnecting

NoMachine Enterprise Desktop supports the **screen blanking** feature: when active, the local user will see a black screen on the physical monitor while somebody is connected from remote to the physical desktop. Operations made on the physical screen are not shown and the local user cannot interact with the desktop until the remote user logs-out. Control is given back to the local user once the remote user has logged off. Screen blanking is available for physical hosts, it is not supported on virtual machines since it has effect on the physical monitor

You can activate the screen blanking feature on the Enterprise Desktop host machine **from the GUI:**

in the Server preferences -> Security panel select the 'Blank the physical screen when somebody connects' option

or **in the server configuration** file, server.cfg.

Uncomment and set:

[EnableScreenBlanking 1](#)

NOMACHINE	NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis	N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell	Last modified: 2019-05-24	Amended: A

To disable screen blanking, set:
[EnableScreenBlanking 0](#).

Then restart the server to make this change effective:

```
nxserver --restart
```

The screen blanking feature can be used in conjunction with the **automatic lock of the remote screen**. Even if the user didn't lock the screen before disconnecting by NoMachine, as soon as the screen is unblanked, the system lock screen will be activated automatically to keep the remote desktop protected even when the computer is running unattended.

You can enable the automatic remote screen lock **from the GUI** in the Server preferences -> Security panel select the 'Lock the physical screen on disconnect' option or **in the server configuration** file, server.cfg.

Uncomment and set:
[EnableLockScreen 1](#)

To disable the automatic screen lock, set:
[EnableLockScreen 0](#)

Then restart the server to make this change effective:

```
nxserver --restart
```

TIP



For versions previous than v. 6.1:
The option to manage the screen blanking from the server User Interface was named 'Lock the physical screen when somebody connects' and the server configuration key was: [EnableScreenLock](#). The possibility to automatically lock the remote screen when the user disconnects was not available.

12.2. Configuring Interaction Level to the Physical Desktop

To forbid users to interact with the desktop once connected set in the server configuration:
[PhysicalDesktopMode 0](#)

In this way, the connected user will access the physical desktop in view-only mode.

To allow interaction instead, ensure to have:
[PhysicalDesktopMode 1](#)

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

12.3. Configuring Users and Authorization for Connecting to a Physical Desktop

Always request the desktop owner's authorization (default)

To request for the explicit authorization of the desktop owner before connecting the user, be sure that the following key is set in the server configuration. The authorization is requested when the connecting user is different from the desktop owner and is not a trusted user.

[PhysicalDesktopAuthorization 1](#)

Make a user trusted

To allow a restricted number of users to connect to the physical desktop without explicit authorization, assign the 'trusted' flag to a new system user:

```
nxserver --useradd --system --trusted physical
```

or edit an existing account:

```
nxserver --useredit --trusted physical
```

Restrict access to specific users

It's possible to limit the access to the physical desktop to the desktop owner, system administrators, NoMachine administrators and trusted users by setting in the server configuration:

[PhysicalDesktopSharing 2](#)

Never request the desktop owner's authorization

To allow **all users** connecting to the physical desktop without explicit permissions, set in the server configuration:

[PhysicalDesktopAuthorization 0](#)

12.4. Configuring User's Ability to Disable Accepting Connections

By default, the owner of the physical desktop, either sit in front of the computer or connected to the physical desktop via NoMachine, has the possibility to switch off/on the sharing of the screen at any moment.

This can be done via the NoMachine Monitor (click on the !M icon in the system tray to open it) and the 'Accepting connection is enabled/disabled' item in the menu.

When 'Accepting connection' is disabled, nobody can connect to that desktop by NoMachine. This setting lasts until the desktop owner changes it again. It persists also when the user physically is logged-out or closed the NoMachine connection. It's therefore strongly advisable to be very careful when disabling accepting connections from remote, since it will be no longer possible to reconnect to the desktop via NoMachine once the current session is closed.

As administrator, you can override user's settings and forcibly enable or disable the screen sharing

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

for the given user. The user, however, will be still able to change it from the !M Monitor menu:

```

nxserver --useredit USERNAME --screensharing yes

or:

nxserver --useredit USERNAME --screensharing no


The screensharing flag can be set also when creating the user:

nxserver --useradd USERNAME --screensharing yes|no

To view the current users' settings:

nxserver --userlist --screensharing yes|no

```

TIP 

If 'Accept connection' is disabled and you cannot reconnect to the desktop via NoMachine, re-enable accepting connections by command line:

```
/etc/NX/nxserver --useredit USERNAME --screensharing yes
```

Removing the 'Accept connection' item from the !M menu

To prevent users from being able to switch 'Accept connection' off and disable the sharing of their screen, set the following key in the node configuration file:

[EnableAcceptingConnection 0](#)

This will hide the 'Accepting connection' item from the Monitor menu.

13. Device Sharing, Copy&Paste and File Transfer

The Enterprise Desktop permits users to access and share their devices and resources from local to remote and vice-versa. Disks, printers, USB devices and more can be connected inside the session to easily access them from both client and server side. At present device sharing is not available with web sessions and requires to connect by NoMachine client.

Two-ways copy and paste is fully supported. Web sessions implements the NoMachine virtual clipboard provides for copying text from/to the session running in the browser and the local computer.

Download/upload files from the session to the local computer and vice-versa is also fully supported in client and web sessions, as well as drag and drop of a file from remote to local and from local to

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

remote.

By default device sharing, copy&paste and file transfer are always permitted. You can however completely disable any of these services or disable it only partially, for example to prevent users from sharing their local printer in the NoMachine session but permitting them to use the remote printer.

13.1. Connecting Devices

NoMachine implements a self-contained infrastructure for making available physical and logical devices over the network from local to remote or vice-versa.

The NoMachine infrastructure for device sharing ensures that all services work out of the box without the need for any additional change or configuration. It is possible to connect disks, printers, USB devices, network port and smartcards.

Connecting devices is supported only by NoMachine client (web sessions don't support that). Devices can be connected through the NoMachine menu within the session (ctrl+alt+0 to open it). Connected devices can be disconnected during the life of the session and reconnected later. If option 'Export this *deviceName* at session startup' is checked in the menu panel, this device is automatically reconnected at the next session start-up.

Disabling device sharing

You can disable selectively the possibility to share a device

from the GUI

in the Server GUI -> Devices panel

or in the node configuration file

by editing the corresponding keys. The manual configuration permits also to limit only oneway of service, for example forbid to connect a local printer to remote. The next paragraphs deal with manual node configurations in detail.

The available devices are:

Devices	Configuration	Technical details
Disks	Local and remote disks can be connected and disconnected during the life of the session and navigated by file browsing. A disk connected as 'Public' is available to all users accessing that desktop. A private disk is available only to the user who connected it. Administrators can configure paths on the server where public and private disks will be mounted as well as specifying which disks on the server can be made available to users.	This service relies on the NoMachine File-system Server (nxfsd) and NoMachine File-system Adapter driver on Windows. On Mac it uses the nxfuse extension whilst on Linux it uses FUSE, installed on the system by default. The nxf and nxfserver programs are used on all systems to mount disks.
	Local and remote printers can be connected at any time (bi-directional printing). A connected printer is listed among the available printers when	This services relies on the NoMachine Device Server service and the NoMachine Printer Adapter driver on

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

Printers	printing a document or similar. A printer can be connected to be 'Public', i.e. available to all users connected to that desktop, or private, for a specific user. It can be also configured to be the default printer.	Windows. On Mac and Linux it uses the CUPS infrastructure present on the system. In this last case, a printer can be exported to the server only if the connected user is in the lpadmim group.
USB devices	USB devices such as disks, pendrives, webcam etc... are forwarded through the network. For example, when a USB device is forwarded from local (where the player is running) to remote, it becomes available on the remote side only.	This service is based only on the NoMachine USB Server (nxusbd) and drivers (NoMachine USB Hub, NoMachine USB Adapter and NoMachine USB Host Adapter on Windows, nxusb.ko kernel module for Linux and nxusb.kext for Mac) and doesn't require external tools.
Network ports	Service ports (such as Samba, CUPS, FTP, SSH, telnet and others) can be made available from local to remote and vice-versa via a virtual network interface.	This service uses the NoMachine Device Server and the NoMachine VPN Adapter driver on Windows and Mac. On Linux it relies on a NoMachine tool plus a standard driver.
Smart Cards	A smartcard reader can be forwarded from client to server side and makes smartcard authentication available within the session. The server host must support authentication via smartcard.	Support for authentication with smart card has been set-up by relying on the Public Key Infrastructure (PKI) and requires an OpenSC compatible smart card. It can be integrated with Kerberos ticket authentication and ticket forwarding.

13.2. Disks

NoMachine allows access to local and remote file systems from within the session through the SSHFS file-sharing protocol and by means of FUSE, a technology to implement a fully functional filesystem in a userspace program.

Connected folders and disks can be disconnected during the life of the session or left as they are.

By default, all disks from the server are available to be connected to the end-user's machine. However you can specify a set of disks and folders by editing a proper value for the [DiskSharingList](#) key in the node configuration file. The default value is: all. Alternatively, you can specify a list of comma-separated directories. Note that \$(HOME) and \$(USER) are accepted values.

For example on Mac you might edit the node configuration file and specify:
[DiskSharingList \\$\(HOME\)/Volumes/TimeMachine](#)

Connecting public disks

Disks from the end-user's machine can be connected on the server in 'Public' or 'Private' mode. By default public disks are exported from player to "\$(PUBLIC)" directory on the server, where \$(PUBLIC) is:

/Volumes on Mac

/media on Linux

C:\Users\Public on Windows Vista/7/8/8.1/10

%ALLUSERSPROFILE% on Windows XP

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

You can specify a different path by un-commenting and editing the [DiskSharingPublicBasePath](#) key in the node configuration file.

Note that \$(USER) is an accepted value that can be also concatenated to specify the path to a directory, for example "/tmp/\$(USER)".

The target directory must exist on the system!

Disabling Disks' Connection

To forbid disk and filesystem sharing, uncomment and set a proper value for the [EnableDiskSharing](#) key in the node configuration file:

client The filesystem on the client can be connected to server side and accessed from the session.

server The filesystem on the server can be connected to the end-user's machine and accessed through the whole life of the session.

both Client and server filesystem can be connected to remote and local sides respectively.

none Neither client or server filesystem can be connected.

For example, to forbid connecting disks from remote to local side, set in the node configuration: [EnableDiskSharing client](#)

13.3. Printers

The printers sharing infrastructure integrates client-side printers with the server-side printing subsystem and vice-versa. Printers available on the client machine can be shared and used within the session as well as printers on the server side which can be made available on the end-user's machine.

Connected printers can be disconnected during the life of the session or left as they are. In this case, they are automatically shared at the next session start-up.

On Linux and Mac this service uses the CUPS infrastructure present on the system. With CUPS 1.4 or later, to ensure that users are able to connect a printer from local to their NoMachine session on Linux or Mac, it's necessary that the user already belongs to the CUPS System Group on the NoMachine server host. That's because, to add a printer to the CUPS system, the 'lpadmin' command line tool has to be executed by a user who belongs to the CUPS's System Group, which can be for example 'lpadmin' on Ubuntu, 'sys' on Fedora, RHEL and CentOS distributions and '_lpadmin' on Mac.

Disabling Printers' Connection

To forbid printer sharing it is necessary to uncomment and set a proper value for the [EnablePrinterSharing](#) key in the node configuration file:

client Printers on the client can be connected to server side and made available within the session.

server Printers on the server can be connected to the end-user's machine.

both Client and server printers can be connected to remote and local sides respectively.

none Neither client or server printers can be connected.

For example, to forbid a server-side printer to be connected to the end-user machine, set in the node configuration:

[EnablePrinterSharing client](#)

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

13.4. USB Devices

This service creates a USB tunnel between client and server to forward devices over the network such as hard disk, web cams, barcode readers, and pen drives from local to remote desktops and vice-versa.

Disabling USB Forwarding

To forbid USB device sharing it is necessary to uncomment and set a proper value for the [EnableUSBSharing](#) key in the node configuration file:

client USB devices on the client can be forwarded to server side and made available within the session.

server USB devices on the server can be connected to the end-user's machine.

both Client and server USB devices can be connected to remote and local sides respectively.

none Neither client or server USB devices can be connected.

For example, to avoid that users can forward a USB devices from the server to its own machine, set in the node configuration:

[EnableUSBSharing client](#)

13.5. Network Ports

NoMachine can create virtual network interfaces and establish a bridge between local and remote sides or vice-versa to provide transparent access to network resources.

This service allows access to any of the default network servers like Samba, CUPS, FTP, SSH and Telnet or any other type, for example a MySQL server.

Connecting a Samba server allows access to resources on that server host via the SMB/CIFS protocol. Connecting a local CUPS server to the remote side allows mounting of printers (local to the user) on that remote CUPS subsystem so that files can be printed on the remote side via the IPP protocol.

Some typical examples of usage:

Print to remote printers from the session

If you have a Linux or Mac machine you can add the local CUPS server via the player toolbar. Choose to add a local server and select CUPS. In this way all printers that are available on your side will be available also on the server and you can print all your documents via the native CUPS (IPP) protocol.

Access a remote host not in your Network Neighborhood

If the remote host has a Samba server, you can add it via the player toolbar. Choose to add a remote server and select Samba as server type. Once that Samba server is added, the remote host shows up in your local Network Neighborhood. You can then connect to remote folders via SMB/CIFS protocol as if that host was in your local network.

Make available a client side HTTP server

You can add your local HTTP server via the player toolbar and make it available on the remote host where your session is running. In this way you can develop and test your web application directly inside the session, without the need for sharing or moving files from remote to local.

Connect to MySQL server behind a firewall

You can choose to add a remote server via the player toolbar. Select 'Custom' and specify MySQL and

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

the port for the MySQL server, by default 3306. Once done, you can connect to that MySQL server via the MySQL client installed on your PC.

Disabling Network Port Forwarding

To forbid network server sharing it is necessary you uncomment and set a proper value for the [EnableNetworkSharing](#) key in the node configuration file: **client** Network servers on client side can be connected and made available within the session.

server Network server on the server side can be connected and made available on the end-user's machine.

both Network servers from client and server side can be connected to remote and local sides respectively.

none Neither client or server side network servers can be connected.

For example, to forbid users from connecting their local ports to the server, set in the node configuration:

[EnableNetworkSharing server](#)

13.6. Smartcard Readers

When the smartcard reader plugged into the enduser's host is forwarded to the server host, the smartcard authentication is made available inside the session. It can be integrated on with Kerberos Ticket system for example for implementing single sign-on (SSO).

Disabling Smartcard readers' Forwarding

You can enable or disable support for smartcard forwarding by uncommenting and setting the [EnableSmartcardSharing](#) key in the node configuration to 1 or 0 respectively.

To disable it set in node configuration file:

[EnableSmartcardSharing 0](#)

13.7. Copy and Paste Operations

By default users can copy and paste from local to the session and vice-versa.

You can configure the server to limit such operations by setting proper values in the configuration file as explained below.

Limiting copy & paste operations

To forbid copy & paste partially or totally, uncomment and set a proper value for the [EnableClipboard](#) key in the server configuration file:

client Content copied on the user's side can be pasted inside the session.

server Content copied inside the session can be pasted on the user's side.

none No copy and paste operations are allowed.

both Two-way copy and paste operations are allowed.

Limiting the Clipboard Buffer

By default, the clipboard buffer is unlimited. If you want, for example, to limit the clipboard buffer to

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

4MB, you have to uncomment and set the following key (value is expressed in bytes) in the node configuration file:
[ClipboardBufferLimit 4194304](#)

13.8. Transferring Files

When a user is connected to the desktop, they have the possibility to transfer files by using the Connection Monitor tool from the system tray within the session. The user can transfer a file from their own PC to the remote host where the session is running and vice-versa. If multiple users are connected, each of them can send a file to a specific user or to all connected users. Drag and drop of a file is also supported

You can manage file transfer
from the GUI

In the Server GUI -> Transfers panel

or **via node configuration**.

Disabling File Transfer

To forbid file transfer you have to uncomment and set a proper value for the [EnableFileTransfer](#) key in the node configuration file:

client Files can be transferred from client machine to the server.

server Files can be sent from the server to clients.

both Client and server files can be transferred on remote and local respectively.

none Neither client or server files can be transferred.

For example, to forbid users from transferring a file from the server to their PC:

[EnableFileTransfer client](#)

14. Multimedia and Session Recording

14.1. Supporting Audio and Microphone

On Linux, NoMachine audio framework is integrated with PulseAudio sound server. If PulseAudio is not available on the system, NoMachine is able to use ALSA (Advanced Linux Sound Architecture). This is automatically managed by the NoMachine server so that multimedia support can work out of the box without the need for any configuration. If both PulseAudio and Alsa are available, the administrator might want to configure the node to use one or the other.

On Windows 10,8,7 and Vista NoMachine's audio system perfectly integrates with the Windows media framework. On XP instead, NoMachine relies on its own driver, the NoMachine Audio Adapter. For

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

microphone support NoMachine always uses the NoMachine Microphone Adapter driver.

On Mac, NoMachine installs and uses its own virtual drivers to support audio and microphone seamlessly.

Disabling or Setting Audio Support

To disable audio and microphone support, uncomment and set the [AudioInterface](#) key to 'disabled' in the node configuration file:

[AudioInterface disabled](#)

On Linux it is possible to define whether PulseAudio Server or ALSA has to be used by setting [AudioInterface](#) key to 'pulseaudio' or 'alsa' respectively. For example:

[AudioInterface pulseaudio](#)

Accepted values on Windows and Mac are instead 'nxaudio' or 'disabled'.

14.2. Recording your Screen

NoMachine permits to record in a video all activities made inside the session or on the desktop. To start the recording of the session, users should open the NoMachine menu inside the session (ctrl+alt+0) and click on the 'Recording' button icon to access the Recording panel. From this panel it's possible to open the recording bar, change audio and video quality and open the recording directory to access all recorded files. Session recording is not available with sessions on the web.

To register activities made on the desktop, start the recording from the !M icon menu in the system tray of the Enterprise Desktop host and show the Recording bar from there. Desktop activities can be registered on the physical desktop without the need to be connected by NoMachine.

Recorded files are saved by default in WebM format and can be played back directly with NoMachine or any other player supporting that format. Video streams can be encoded only with VP8 or H.264 when supported. Recorded files are saved by default on the user's device in the NoMachine directory under the 'Documents' directory.

Disabling session recording

To prevent users from recording their session activities, edit the node configuration to set:

[EnableSessionRecording 0](#)

Disabling desktop recording

To prevent users from recording desktop activities, even when physically logged into the Enterprise Desktop host, edit the node configuration to set:

[EnableLocalRecording 0](#)

15. Automatic Updates

The Enterprise Desktop, as well as the other NoMachine client and server products, periodically

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

checks NoMachine repositories (by default every two days) to verify if updates are available and will prompt a dialog informing the user that a new version is available.

It will **never** automatically update the current installation. Also the download in background of a new software version will not lead to an automatic update of the current installation.

A separate guide, available at: <https://www.nomachine.com/all-documents> deals specifically with all the possible options for the automatic software updates.

16. Logging Facilities

To retrieve logs by using the NoMachine tools, please refer to guides available in the Configuration section at: <https://www.nomachine.com/all-documents>.

TIP



When debug mode is enabled, server logs may increase consistently. It's suggested to keep debug level only for the time necessary to reproduce the problem and collect logs.

16.1. Using the System Logging Facilities

By default the nxserver, nxwebplayer/nxwebclient and nxnode programs log to the file defined in the SystemLogFile key in their configuration files (server.cfg for nxserver and nxwebplayer/nxwebclient and node.cfg for nxnode).

It's possible to configure these applications to log to the system log file instead. Edit the server.cfg and node.cfg files, uncomment and set:

[EnableSyslogSupport 1](#)

Then restart the server and all services to make the change effective:

```
nxserver --restart
```

16.2. Redirecting Logs to a Custom File

You can redirect logs of nxserver, nxwebplayer/nxclient and nxnode programs to a custom file by uncommenting and setting the path to that file in the SystemLogFile key available in the server and node configuration files. By default this key is set to:

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

`SystemLogFile /usr/NX/var/log/nxserver.log`

Change it to point to a different file, for example:

`SystemLogFile /tmp/NX.log`

TIP



The custom file must be accessible (writable) to the 'nx' user and to the connected user.

16.3. Configuring the Automatic Clean-up of Session Directories

In its default configuration, the Enterprise Desktop removes the session directory from the 'node' directory in the NoMachine var/log directory once the session has been correctly terminated. The 'node' directory is:

`/usr/NX/var/log/node` on Linux

`%PROGRAMDATA%\NoMachine\var\log\node` on Windows

`/Library/Application Support/NoMachine/var/log/node` on Mac.

You can preserve it, for example for log purposes, by uncommenting and disabling the following key in the node configuration file. In this case, the session directory in user's home/.nx is renamed as T-C*:

`SessionLogClean 0`

16.4. NoMachine Log Rotation

NoMachine supports log rotation for its log files since v. 6.5.6. Once activated, in the default configuration, logs are rotated once per month when they exceed 100MB. If not otherwise specified, NoMachine preserves up to seven rotated files and deletes the oldest ones.

Rotated logs are saved in the following directories:

`/usr/NX/var/log/logrotate` on Linux

`%PROGRAMDATA%\NoMachine\var\log\logrotate` on Windows

`/Library/Application Support/NoMachine/var/log/logrotate` on Mac.

To activate log rotation:

```
nxserver --logrotateadd OPTION
```

OPTION can be any of the following:

`--rotate VALUE`, specify the maximum number of rotated files to be preserved in the logrotate directory. When this number is exceeded, the oldest files are deleted.

`--timeinterval TIME`, specify the frequency of log rotation. Frequency can be specified in seconds or by using the

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

'Daily', 'Weekly', 'Monthly', or 'Yearly' keyword. Rotate logs when the interval of time and the minimum log size is reached.

--minsize VALUE, specify the minimum file size for rotating logs according to the given interval of time. If the minimum size is not reached, logs are not rotated. Value is by default in kilobytes, add M or G to set it in megabytes or gigabytes respectively.

--size VALUE, specify the minimum file size for applying log rotation as soon as the file size is reached, regardless of the frequency set for log rotation.

--compress yes|no, by default each log file is compressed as a gz archive, use '--compress no' to not compress it.

--destination PATH, provide an alternative path where to store the rotated files.

If OPTION is not specified, the default settings will be applied.

By default, log rotation is applied to all NoMachine log files. It's possible to specify which log file should be under log rotation:

```
nxserver --logrotateadd LOG OPTIONS
```

LOG can be any of the following file name:

nxserver.log

nxerror.log

nxd.log

nxservice.log (on Windows only)

nxwebclient.log

nxhtd-error.log

nxhtd-access.log

If OPTION is not specified, the default settings will be applied.

To edit parameters set for log rotation:

```
nxserver --logrotateedit LOG OPTION
```

To list current settings for log rotation:

```
nxserver --logrotatelist
```

To delete all settings for log rotation:

```
nxserver --logrotatedel
```

To delete log rotation settings for a specific log file:

```
nxserver --logrotatedel LOG
```

Some examples:

Rotate all logs monthly (the minimum size is the default 100MB):

```
nxserver --logrotateadd --timeinterval Monthly
```

Rotate only nxserver.log (which usually has the most relevant size) weekly if it exceeds the default size of 250MB:

NOMACHINE		NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis		N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell		Last modified: 2019-05-24	Amended: A

```

nxserver --logrotateadd nxserver.log --timeinterval Weekly --minsize 250M

Rotate nxserver.log when it exceeds 250MB:

nxserver --logrotateadd nxserver.log --size 250M

Rotate the given logs weekly when they exceed 250MB and save the rotated files in a specific path:

nxserver --logrotateadd nxserver.log --timeinterval Weekly --minsize 250MB --destination /var/log/
nxserver --logrotateadd nxerror.log --timeinterval Weekly --minsize 250MB --destination /var/log/

```


It's possible to force log rotation at any moment. This doesn't require to enable it. To apply log rotation to all files or to a given log only:

```

nxserver --logrotate LOG OPTIONS

OPTION can be any of the following options:
--compress yes|no, by default the log file is compressed as gz archive, use '--compress no' to not compress it.
--destination PATH, provide an alternative path where to store the rotated files.

```

TIP 

To debug a problem easily reproducible, it could be helpful to clean up logs with 'nxserver --logrotate', activate the debug log level with 'nxserver --debug --enable all', reproduce the problem, collect logs with 'nxserver --debug --collect' and finally restore informational log level with 'nxserver --debug --disable all'.

17. Setting-up a Centralized Access to Multiple Enterprise Desktop Servers

If you own multiple installations of Enterprise Desktop, you may need to provide a single point of access to all of these servers. This can be done by installing NoMachine Cloud Server on a dedicated host and add each Enterprise Desktop to it.

In this way, users will connect to the hostname/IP of the Cloud Server and will be redirected to the appropriate Enterprise Desktop or, depending on the Cloud Server configuration, will be able to choose it manually.

You may also configure the NoMachine centralized infrastructure to make each Enterprise Desktop to accept or refuse direct connections to its host.

To grant high available access to this centralized system, it's possible to add a second Cloud Server to the first one and set-up a failover cluster.

NOMACHINE	NoMachine Enterprise Desktop - Installation and Configuration Guide	
Prepared by: Silvia Regis	N°: D-705_003-NMC-NTD	
Approved by: Sarah Dryell	Last modified: 2019-05-24	Amended: A

17.1. Federating the Enterprise Desktop Under a Cloud Server

In order to federate an Enterprise Desktop under a Cloud Server, connect to the Cloud Server host as a NoMachine administrator and use the graphical interface to add the server.

Otherwise, execute on the Cloud Server host the 'nxserver --serveradd ' command.

For more advanced options, such as setting up the protocol (NX or SSH) and method to be used for forwarding the connection from client to the Enterprise Desktop, please refer to the NoMachine Cloud Server Guide available in the Document sections: <https://www.nomachine.com/all-documents>
