

Net Monitor for Employees Professional

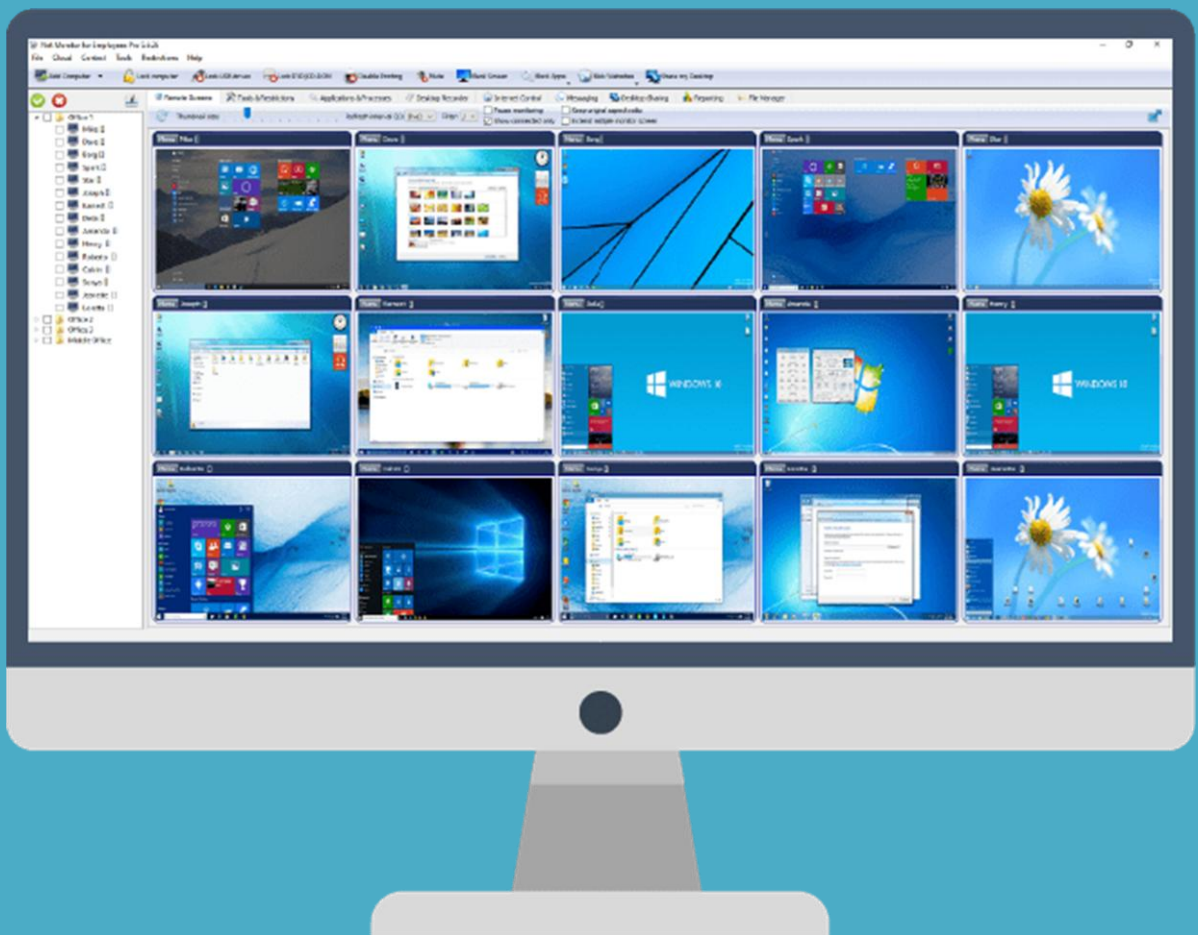


Table of Contents

1. Quick Start and Product Overview.....	4
Quick Start.....	4
Major Benefits.....	4
Main Features	4
2. Installation and Deployment.....	6
Package Types and Required Ports.....	6
2.1 Install the Monitoring Console.....	7
2.2 Install the Net Monitor for Employees Pro Agent on a Local Network	8
2.3 Install the Application in the Cloud	12
2.4 RDP Session Monitoring for Terminal Services.....	18
2.5 ChromeOS and Chromebook Employee Monitoring.....	19
3. Using the Monitoring Console	22
3.1 Add Computers Manually.....	22
3.2 Add Computers from Cloud	24
3.3 Scan Network for Installed Agents	25
3.4 Add Group of LAN Computers	26
3.5 Remote Computers List	27
3.6 Import and Export Computers (CSV, Tab-Delimited, Excel)	28
4. Live Monitoring and Remote Screens	29
Typical Use Cases	29
Remote Screens Overview	29
Toolbar Controls	29
Camera Tiles.....	30
Recommended Workflow	30
5. Control Tools and Restrictions.....	31
5.1 Tools Tab — Immediate Actions	31
5.2 Restrictions Tab — Persistent Restrictions.....	33
5.3 Time Restrictions Tab — Daily Computer Time Limits	33
6. Applications and Process Restrictions	35
Applications Tab	35
Processes Tab	36
Blocking Applications Tab.....	37

7. Recording, Logging, and Reporting	38
7.1 Employee Screen Recording with Computer Screen Recorder	38
7.2 Employee Audio Monitoring with Computer Audio Recorder	39
7.3 Recording External Storage	41
7.4 Employee Activity Tracker and Monitoring Reports	49
8. Internet Control, Messaging, and Desktop Sharing.....	52
8.1 Internet Blocking Software for Employee Computers.....	52
8.2 Employee Messaging Software for Remote Computer Alerts	53
8.3 Share Desktop for Remote Presentation and Training	54
9. File and Administrative Tools	56
9.1 Remote File Manager for Employee Computers.....	56
9.2 Remote Terminal CMD PowerShell Bash.....	58
9.3 Remote System Information and Computer Inventory	59
10. Remote Desktop Control	61
Remote Desktop Control	61
Start Session From Object Menu	61
Remote Control Window Controls.....	62
Session Notes.....	62
11. Mobile Console for iOS and Android	63
11.1 Install Agent	63
11.2 Find and Add PCs Where Agent Is Installed	64
11.3 Manually Add Computers	65
11.4 Computer List View.....	66
11.5 Action Menu	67
11.6 Remote Screens View	67
11.7 Tools View	68
11.8 Processes View	69
11.9 Remote Control	70

1. Quick Start and Product Overview

Net Monitor for Employees Pro lets you see what everyone is doing without leaving your desk. You can monitor the activity of all employees and share your screen with employee PCs, making demos and presentations easier.

Quick Start

1. Install all agents on computers that you want to monitor.
2. When installing each agent, choose a password that will later be used in the console for adding the computer.
3. Open the used port, TCP 4495, on all firewalls.
4. Install the console on the computer from which you want to monitor or administer other computers.
5. When the console is installed, add every computer using the password you used during agent installation.
6. After computers are added, start using the application.

Major Benefits

- Installation and use of the application is very easy since all of the functions can be accessed with a few mouse clicks.
- You have complete control over what employees are doing.
- This application provides you with a live picture of the employee computer screens.
- You can make the presentation by showing your live screen to students or presenting student screen to others.
- Application allows you to take over the employee computer by controlling its mouse and keyboard.
- The employee computers' screens are represented in the table with a customizable number of rows as thumbnails.
- Schedule employee computers desktop recording to JPEG or MPEG files.
- Schedule audio recording of microphone.
- Monitor and record attached camera.
- Execute several actions on all employee computers with one click.
- Execute interactive terminal commands on remote computers.
- Get detailed information about the remote computer.
- Block applications and Internet access.
- Log user activity.
- Log visited web pages.
- Log used applications.
- Log keystrokes (key-logger).
- ...and much more - see feature list and screenshots.

Main Features

- Displaying a live picture of an employee computer.
- You can take control of an employee computer by controlling its mouse and keyboard.
- More employee monitor screens can be displayed in a table.
- Computers can be organized in computer groups (e.g. classrooms).
- An employee monitor screen can be zoomed to an actual size.
- The name of the connected user is displayed.
- Record employee computers screens to JPEG or MPEG files.

- Record microphone audio.
- Execute CMD shell.
- Get information about the remote computer (network info, user accounts, installed applications, WLAN profiles, Outlook profiles, other network attached devices).
- Show your desktop to students or show student desktop to students.
- Power on/off, restart, hibernate, suspend employee computers.
- Log off desktop users.
- Lock workstation.
- Clear desktop.
- Control screen-saver.
- Block Internet.
- Block applications.
- Mute employee computers.
- Limit employee computers audio volume level.
- Disable printing.
- Disable Ctrl+Alt+Del.
- Blank screen.
- Start program on employee computers and see the output.
- Open web page on employee computers.
- Multi-monitor support.
- Control over running processes and applications.
- You can lock selected employee computers.
- You can display a message on selected employee computers.
- When lower bandwidth is required, the refresh interval can be enlarged.
- Automatic connection to an employee computer is optional.
- Settings for the agent are encrypted and password protected.
- Connection to an employee computer is password protected.
- Access to the monitoring console is password protected. If more users use the same computer, different profiles and access passwords can be set.
- More monitoring consoles can be connected to the same employee computer - you can monitor your students from different locations.
- Agent can be remotely installed.
- Fast user switching is supported.
- Multi-session support for Remote Desktop, Terminal Services, Citrix, and similar environments.
- Console can be used on smartphone or tablet.
- Cloud connection allows monitoring over different networks or Internet.

2. Installation and Deployment

This chapter contains the console, agent, LAN, Cloud, RDP, and ChromeOS deployment procedures.

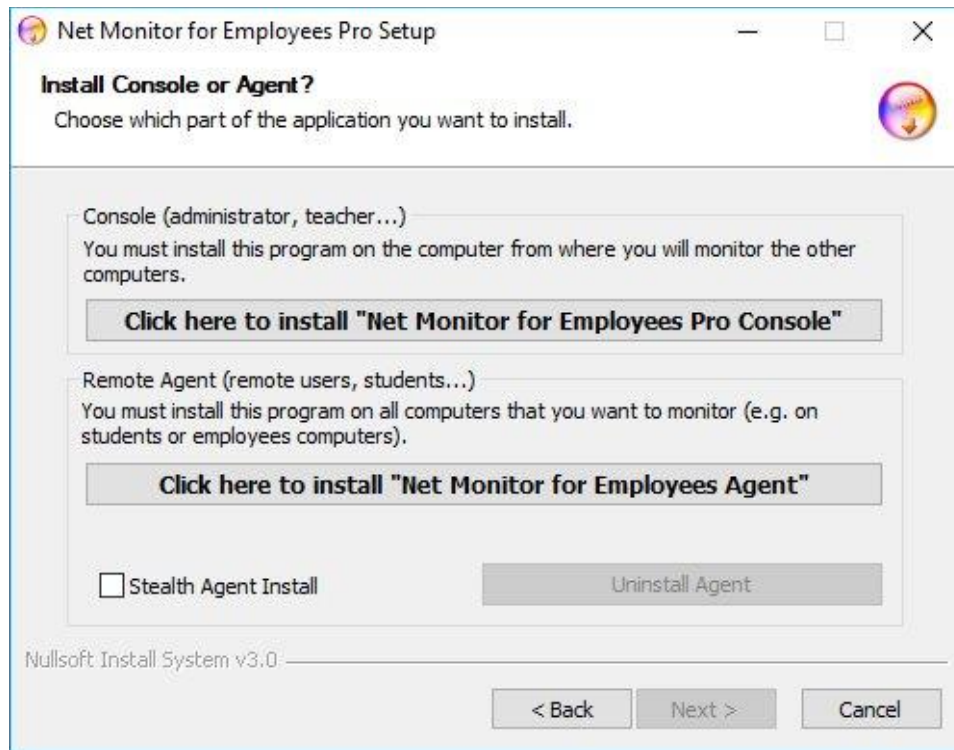
Package Types and Required Ports

Use the package type that matches the operating system and deployment method. The same agent password and configured communication ports are used later when computers are added to the console.

Package / component	Use
Windows Full Package	Desktop package containing console and agent installers.
macOS Full Package	macOS installer package containing console and agent installers.
Linux Full Package	Linux installer package containing console and agent installers.
iOS Console	Mobile console for iOS devices.
Android Console	Mobile console for Android devices.
Windows Agent (MSI) — nmemplpro_agent.msi	Agent package used for Active Directory / MSI deployment.
Windows Console (MSI) — nmemplpro_console.msi	Console package used for Active Directory / MSI deployment.
ChromeOS Agent / Chrome extension	Extension used to monitor ChromeOS / Chromebook devices.
Detail info	Default / recommendation
Agent access password	Choose and remember a password during agent installation; use the same password when adding the computer to the console.
Direct Connection port	TCP 4495 by default; open it on firewalls as needed. Here agent acts as TCP server.
Reverse Connection Server port	TCP 444 by default; open it on the console computer firewall if you plan to use Reverse connection (console acts as TCP server)
Cloud connection	Requires Cloud account and subscription-based Cloud license.
Remote agent installation	Requires Active Directory administrative privileges and works on LAN, WLAN, or VPN; Internet remote install requires VPN.
Terminal/RDP monitoring	Install agent on TS/RDP server and add only the server to console; sessions appear automatically.

2.1 Install the Monitoring Console

Installing Console Manually (Preferred)



Screenshot: Installer option used to install the console or agent.

To install the employee monitoring console, select the first option: Net Monitor for Employees Pro Console.

The Net Monitor for Employees Pro Console must be installed on one or more computers from which you want to monitor the remote computers.

Log in to the computer from where you want to monitor other users. Log in as the user that uses this computer or as administrator. Start the console and type the password that you want to use for accessing the console.

If more users use the same computer, they must all log in to the computer using their accounts and set their own password for the console.

Remote Console Installation over Active Directory

Use the console MSI package named nmemplpro_console.msi for remote deployment over Active Directory.

```
msiexec /i nmemplpro_console.msi INSTALL_LICENSE=Y REGISTRATION_NAME="My Registration Name"  
LICENSE_KEY="2459-xxxx-yyyy-zzzz-000e-278d" /qn
```

Deploy as usual using package nmemplpro_console.msi and specify these MSI properties:

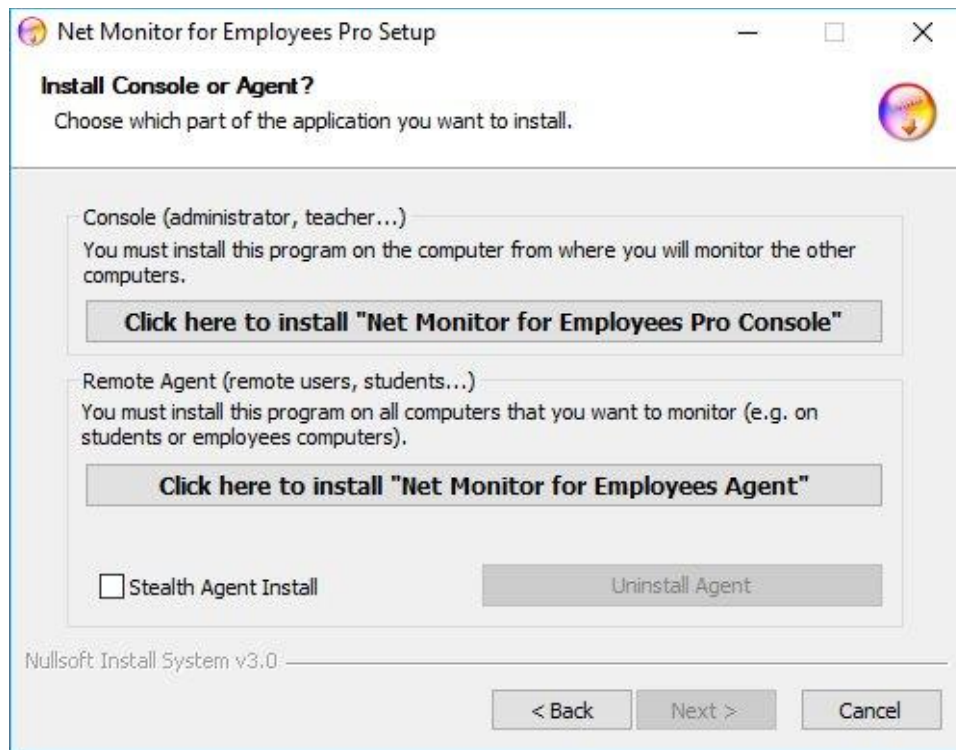
```
INSTALL_LICENSE=Y  
REGISTRATION_NAME=MyRegistrationName  
LICENSE_KEY=MyLicenseKey
```

2.2 Install the Net Monitor for Employees Pro Agent on a Local Network

To start monitoring your employee, install the employee monitoring software in your workplace. The application consists of two modules that must be installed:

- Net Monitor for Employees Pro Console.
- Net Monitor for Employees Pro Agent.

The Net Monitor for Employees Pro Agent must be installed on all remote computers that you want to monitor. To do this, you must have administrative privileges. The agent can be manually or remotely installed.



Screenshot: Select the agent option in the installer.

Manual Installation (Preferred)

To manually install an agent, go to the remote computer and run the installation program. In the first installation window, click the second option to install Net Monitor for Employees Pro Agent. At the end of installation, configure the agent.

Agent can be installed in stealth mode by selecting the Stealth Agent Install checkbox. In this way, no program group is created, the application does not appear in Add/Remove Programs, and no icon is displayed.

Agent Configuration

Agent Configuration

Configuration

Connection Type:

Note:
Using a Cloud connection allows you to monitor your users over the Internet and not only on your local network. This option is charged as a subscription and will open the wizard for creating or selecting a Cloud account.

☒ Use direct connection - console acts as a client (connect via local network - LAN/WLAN) [Default]

☐ Use reverse connection - console acts as a server (connect via local network - LAN/WLAN)

☐ Use Cloud connection (connect via the Internet)

Agent Password (restrict access to this computer):

☐ Change password

Password: Retype password:

Direct connection TCP port:

Reverse connection to the Console:

Console IP or Host: Password: Port:

Agent is stopped.

Screenshot: Agent configuration on a local network.

During installation, type the password that protects the configuration and access to the agent. Select one password and remember it. The default port on which the agent operates is 4495. You can change this port during installation or later on the Advanced Configuration tab. If you use a firewall, open the used port.

Under Connection Security, choose End-to-end encryption (the original built-in encryption) or TLS, the same protocol used to secure web traffic - the console must be set to match, or left on Auto. When TLS is selected, the agent shows the certificate's fingerprint with a Copy button so it can be read or sent to whoever confirms it on the console side, and "End-to-end encrypt traffic also for TLS" is checked by default.

Connection Types

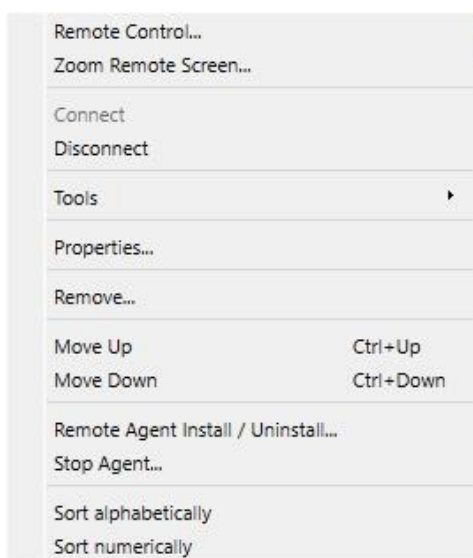
Connection type	How it works	Required port / conditions
Direct Connection	Uses a direct TCP/IP connection between the admin console and agents. The console acts as a client and the agent as a server. Direct connection works if all computers are on the same network or proper routing is configured between subnetworks.	Default TCP 4495 must be enabled for communication.
Reverse Connection	Uses a direct TCP/IP connection between admin console and agents. The console acts as a server and the agent as a client. You need to enable Console Reverse	Default TCP 444 must be enabled for communication.

	Connection Server in the console and specify the console host name or IP to which the agent will connect.	
Cloud Connection	Makes the computer accessible via a cloud connection so it can be monitored over the Internet.	Cloud license is subscription based.

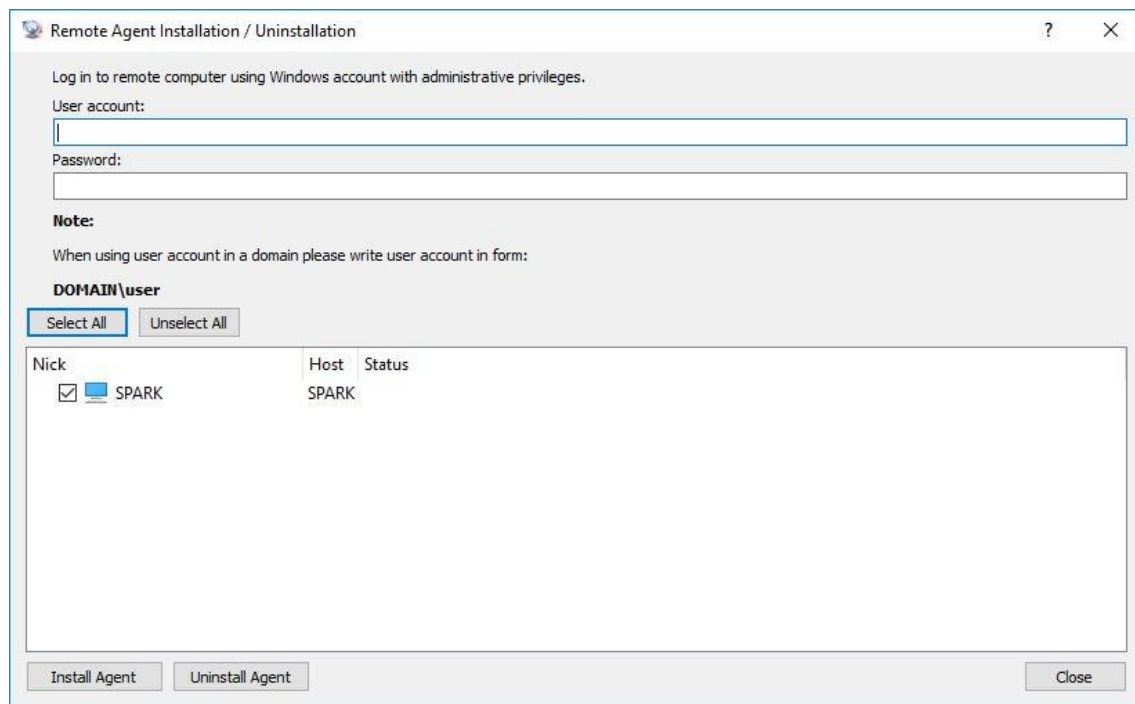
Remote Agent Installation on Windows

Remote agent installation is possible only on NT-based operating systems such as Windows 7, 8, 10, and 11 with administrative privileges. The used port will be automatically opened only on Windows Firewall. On other firewalls, open this port yourself. Remote installation can be done on LAN, WLAN, or VPN. Remote installation over the Internet is not possible unless you use a VPN network.

To start remote agent installation, right-click a computer in the list. The Object Menu appears. Choose Remote Agent Install / Uninstall (Windows). After that, the login screen appears. Enter the user account information on the remote computer that has administrator privileges.



Screenshot: Object menu with remote agent installation option.



Screenshot: Remote Agent Installation / Uninstallation login and computer list.

Remote Agent Installation on Linux (over SSH)

Linux agents can be installed and uninstalled remotely over SSH, from a console running on any operating system (Windows, Linux, or macOS). The console obtains the correct Linux agent files as needed - either bundled with the console or downloaded for this brand - and installs them on the remote computer through an encrypted SSH connection.

Select one or more Linux computers in the list, right-click, and choose Remote Agent Install / Uninstall (Linux). The same command is also available in the File menu.

In the dialog, enter the SSH connection details for the remote computer(s):

SSH user / SSH password - the account used to log in over SSH. Instead of a password you can choose a Private key file for public-key authentication; the SSH password field is then used as the key's passphrase.

SSH port - the port the SSH server listens on (22 by default).

sudo password - installation requires root privileges. Leave this empty if the SSH account is root, or if its sudo password is the same as the SSH password; otherwise enter the sudo password.

Select the computers and click Install Agent or Uninstall Agent. The status and progress are shown for each computer, and the buttons become available again once every computer has finished, so you can adjust the details and retry if needed.

Note: The agent's port is opened automatically only where the ufw or firewalld firewall is active; with any other firewall you must open the port yourself.

Update Agent

If this console has a newer agent version available, you can push it to already-installed agents remotely, without a full reinstall.

To update an agent, select one or more connected computers in the list, right-click, and choose Update Agent... from the menu.

The console sends the new agent files to each selected computer and only replaces the existing files once every new file has been fully and correctly received, so an interrupted or failed update never leaves the agent in a broken state.

Click Run in Background to keep working in the console while the update runs - progress for all selected computers is then shown in the status bar.

Note: The console can only update agents running on a platform (Windows/macOS/Linux) it has agent files for, either bundled locally or available to download for this brand. If neither is available, the update for that agent fails with an explanation instead of guessing.

Uninstall Agent

You can remotely and completely remove an already-installed agent from a computer, without needing physical or file-share access to it.

To uninstall an agent, select one or more connected computers in the list, right-click, and choose Uninstall Agent... from the menu.

The agent is stopped and its entire install folder is removed - including any files or folders the console does not otherwise recognize - so nothing is left behind.

Click Run in Background to keep working in the console while the removal runs - progress for all selected computers is then shown in the status bar.

Note: This permanently removes the agent from the computer. Monitoring for that computer stops immediately and cannot be resumed without installing the agent again.

Remote Agent Deployment over Active Directory Using MSI Package

Use the agent MSI package named nmemplpro_agent.msi for remote deployment over Active Directory.

```
msiexec /i nmemplpro_agent.msi PASSWORD=myAgentPassword /qn
```

Deploy as usual using package nmemplpro_agent.msi and specify the MSI property:

```
PASSWORD=myAgentPassword
```

The myAgentPassword value is the password you want to use.

By default the agent uses end-to-end encryption for its connection to the console. To use TLS instead - the same protocol used to secure web traffic - add the property:

```
USE_TLS=Y
```

When TLS is used, end-to-end encryption is also layered on top of it by default; to use TLS on its own instead, also add TLS_WITHOUT_ENCRYPTION=Y.

Note: Install the Monitoring Console in the same network as employee computers that you want to monitor.

2.3 Install the Application in the Cloud

By installing Net Monitor for Employees Pro to the Cloud, you can perform remote employee monitoring over different networks and the Internet. Install these two modules to start with cloud-supported remote employee monitoring:

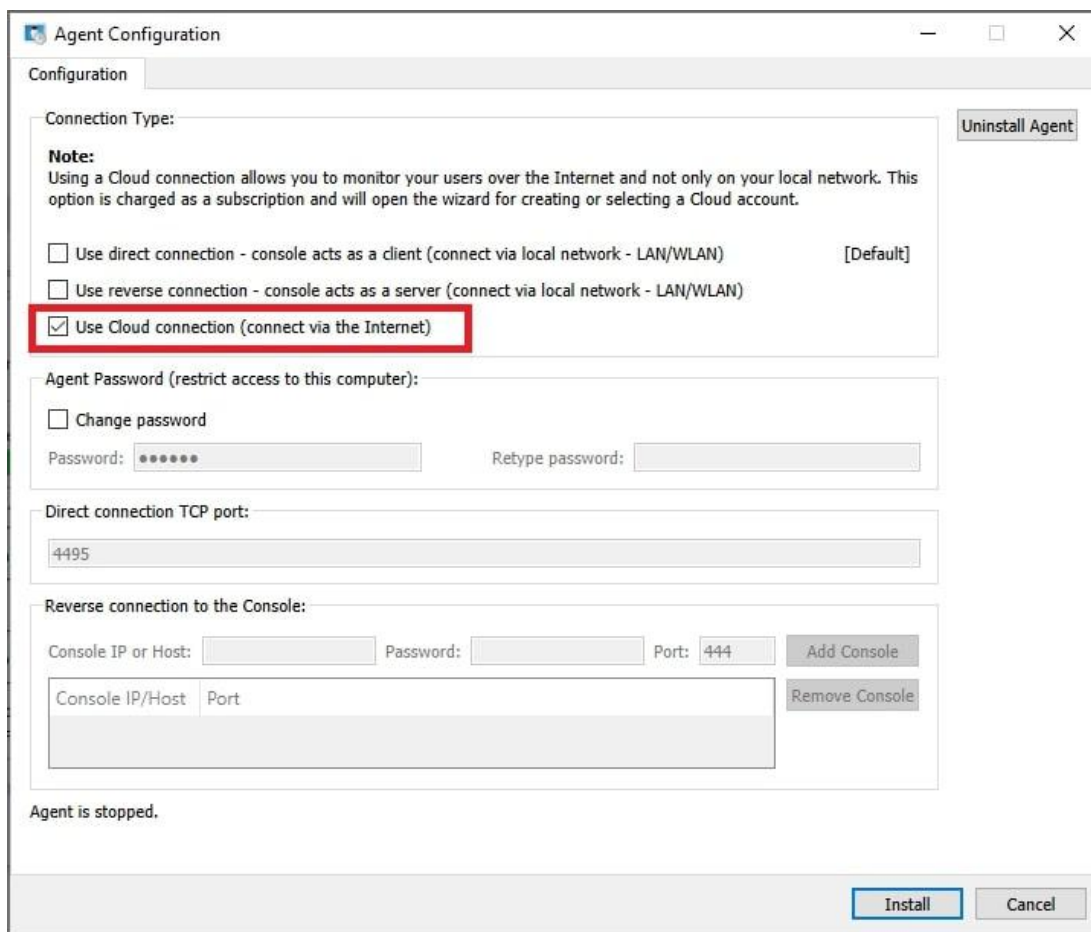
- Net Monitor for Employees Pro Console.
- Net Monitor for Employees Pro Agent.

Installing the Net Monitor for Employees Pro Agent

The agent must be installed on all remote computers that you want to monitor. Administrative privileges are required. The agent can be manually or remotely installed.

To manually install an agent, go to the remote computer and run the installation program. In the first installation window, click the second option to install Net Monitor for Employees Pro Agent. At the end of installation, configure the agent.

Agent can be installed in stealth mode by selecting the Stealth Agent Install checkbox. In this way, no program group is created, the application does not appear in Add/Remove Programs, and no icon is displayed.



Screenshot: Agent configuration with cloud connection option.

During installation, type the password that protects configuration and access to the agent. Select one password and remember it. The default port is 4495 and can be changed during installation or later on the Advanced Configuration tab. If you use a firewall, open the used port.

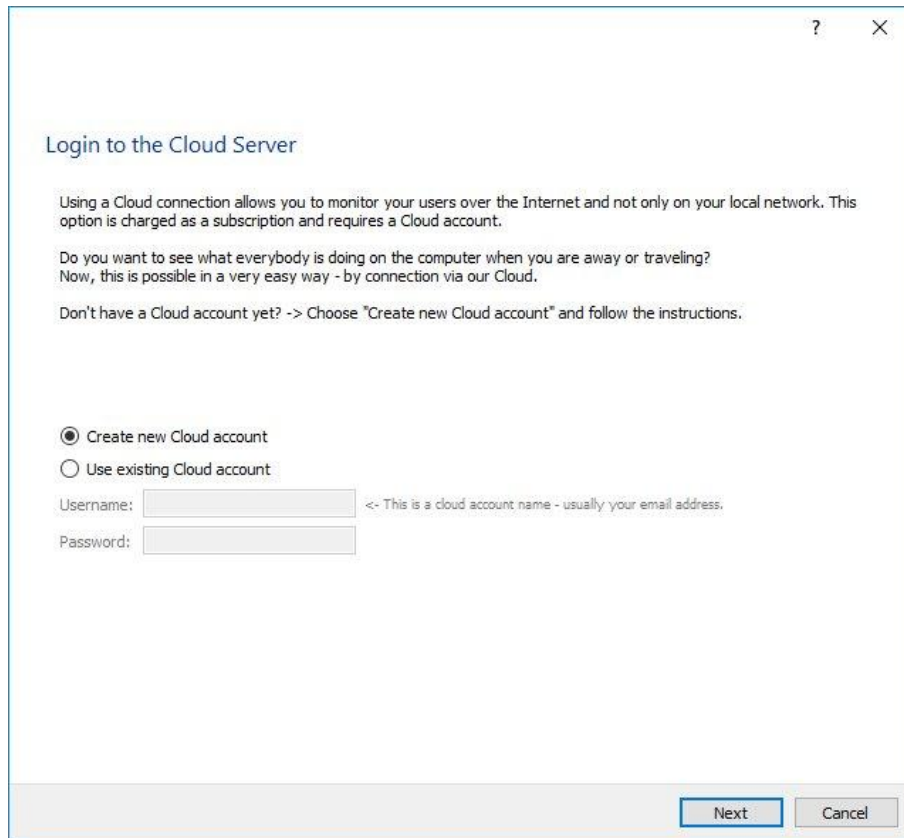
You can choose to make this computer accessible only via Cloud connection by selecting Use Cloud connection, which allows monitoring over the Internet. Cloud license is subscription based.

Create Cloud Account (Needed Only First Time)

If you selected Cloud connection, you will be asked to use an existing Cloud account or create a new Cloud account. If you are creating a Cloud account for the first time, your trial Cloud license will be automatically enabled.

Note: Cloud account can also be created directly from the monitoring console using menu Cloud / Create Cloud account. To monitor your computer over the Internet, you need to have the Cloud account.

If you do not have the Cloud account yet, create it by selecting Create new Cloud account. You will receive an email with account activation code after confirming this step. If you did not receive an email, check the spam folder or contact support. Proceed with installation and enter the account activation code from email.



?

X

Login to the Cloud Server

Using a Cloud connection allows you to monitor your users over the Internet and not only on your local network. This option is charged as a subscription and requires a Cloud account.

Do you want to see what everybody is doing on the computer when you are away or traveling?
Now, this is possible in a very easy way - by connection via our Cloud.

Don't have a Cloud account yet? -> Choose "Create new Cloud account" and follow the instructions.

☒ Create new Cloud account

☐ Use existing Cloud account

Username: <- This is a cloud account name - usually your email address.

Password:

Next Cancel

Screenshot: Cloud login / create-account choice.

Create account on Cloud Server

Using a Cloud connection allows you to monitor your users over the Internet and not only on your local network. This option is charged as a subscription and requires a Cloud account.

With a cloud account you will be able to install the application and log in to the monitoring console.

Please make sure that you are using a valid email address because account activation code will be sent to that address.

Account Name* <- It is recommended that you type your email address here.

Password*

Retype Password*

Email Address* <- Account activation link will be sent to this address.

Retype Email Address*

 <- Enter Captcha

☒ I agree that you can use here provided data to send me all necessary information about my account and this application use.

Screenshot: Create a Cloud account.

Activate Account for Net Monitor for Employees Σ Inbox x

info@networklookout.com

to me ▾

Dear Net Monitor for Employees user,

Thank you for starting a registration with **Net Monitor for Employees** (<https://networklookout.com>).

To complete the registration, you need to activate your account "my_cloud_account".

The application will ask you to enter the account activation code.

To activate your account, please enter the following Account Activation code (use copy/paste):

ba38f061-c47a-4f2b-a888-506b49588dbd

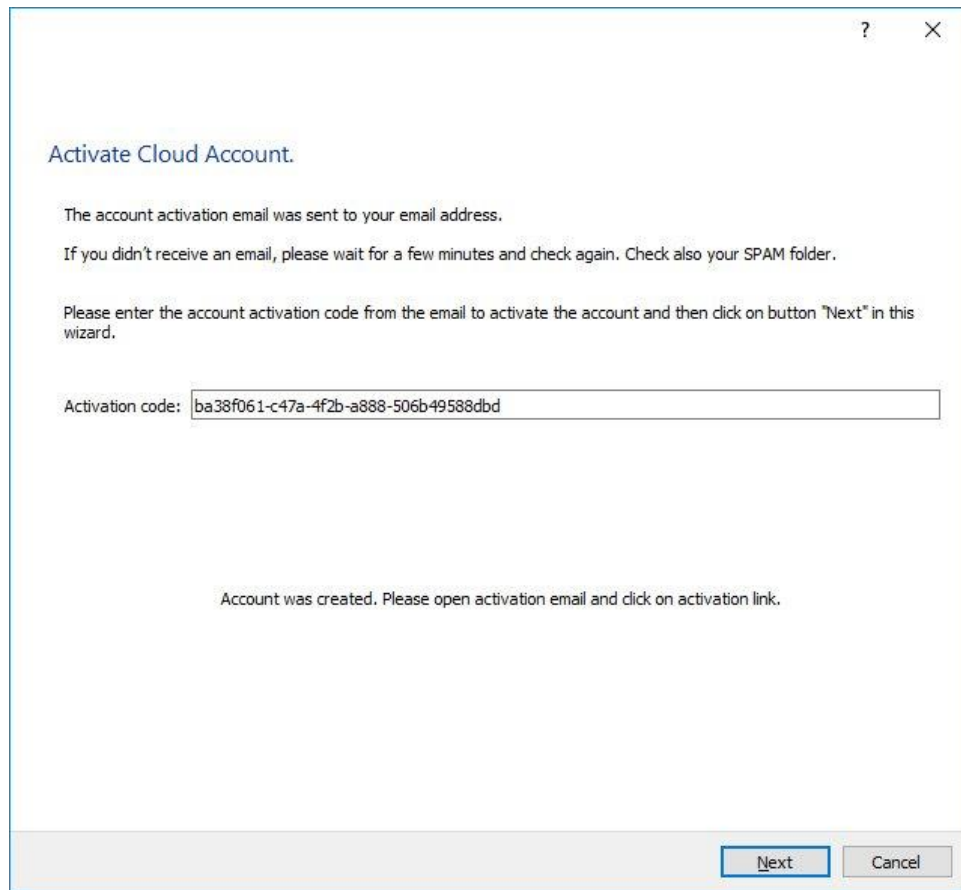
By activating the account you agree that we can use your data to send you all necessary information email to info@networklookout.com.

If you don't activate the account then you will receive one more email reminding you about account ac

Best regards,

Net Monitor for Employees Customer Support

Screenshot: Activation code email.



Screenshot: Activate the Cloud account.

Use Existing Cloud Account

If you already created a Cloud account, choose Use existing cloud account and enter your Cloud account username and password. Click Next and confirm that you want to monitor this computer. After that, your remote computer is added to the cloud and can be added to the console using menu Cloud / Add computers from Cloud.

?

X

Login to the Cloud Server

Using a Cloud connection allows you to monitor your users over the Internet and not only on your local network. This option is charged as a subscription and requires a Cloud account.

Do you want to see what everybody is doing on the computer when you are away or traveling?
Now, this is possible in a very easy way - by connection via our Cloud.

Don't have a Cloud account yet? -> Choose "Create new Cloud account" and follow the instructions.

☐ Create new Cloud account

☒ Use existing Cloud account

Username: <- This is a cloud account name - usually your email address.

Password:

Next Cancel

Screenshot: Use existing Cloud account.

?

X

Add this computer to the Cloud.

If you add this computer to the Cloud then you will be able to monitor it from anywhere and not only on your local network.

Do you want to add this computer to the Cloud?

☒ Yes

☐ No

Next Cancel

Screenshot: Confirm computer is monitored over the Internet.

Remote Agent Deployment over Active Directory Using MSI Package

Remote agent installation is possible by deploying the MSI package over Active Directory. Use package nmemplpro_agent.msi and specify these properties:

```
msiexec /i nmemplpro_agent.msi PASSWORD=my-agent-password CLOUD_ADD=Y CLOUD_ACCOUNT=my-cloud-account  
CLOUD_PASSWORD=my-cloud-password /qn  
  
PASSWORD=my-agent-password  
CLOUD_ADD=Y  
CLOUD_ACCOUNT=my-cloud-account  
CLOUD_PASSWORD=my-cloud-password
```

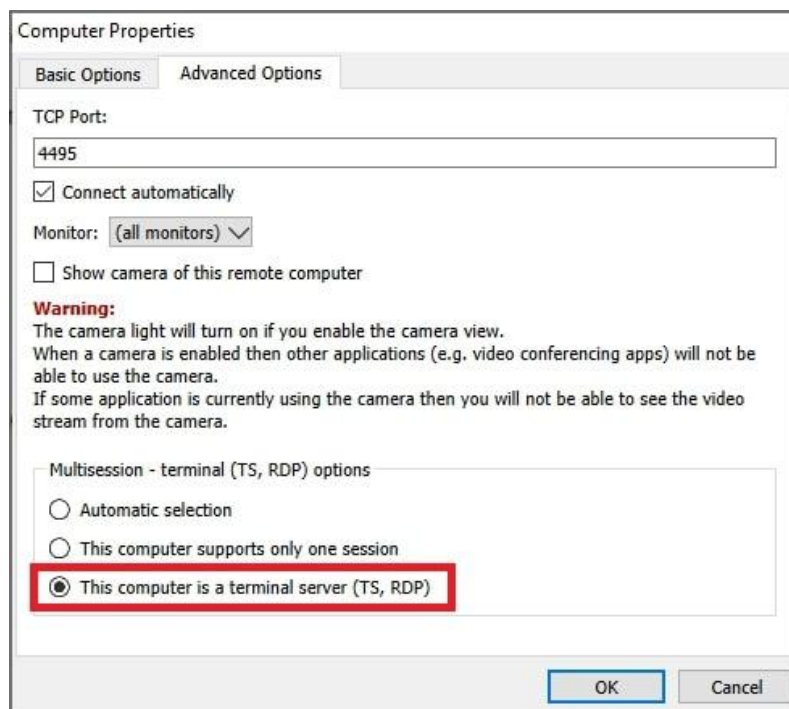
2.4 RDP Session Monitoring for Terminal Services

To monitor employee RDP sessions, install these two modules:

- Net Monitor for Employees Pro Console — can be installed anywhere in your network.
- Net Monitor for Employees Pro Agent — must be installed on the TS/RDP server.

The application can monitor individual TS/RDP sessions. In this case, the agent must be installed on a Terminal Services Server using the same procedure as local network installation. When installing the agent, you can make all TS/RDP sessions accessible also via Cloud connection by selecting Use direct or cloud connection. Cloud license is subscription based.

Add only the server to the monitoring console because sessions appear automatically. When adding the server to the console, select Advanced Options and choose This computer is a terminal server (TS, RDP).



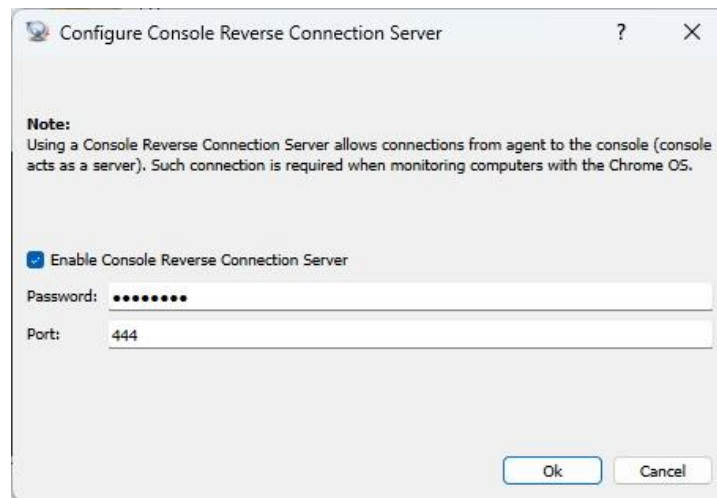
Screenshot: Terminal server / RDP monitoring configuration.

2.5 ChromeOS and Chromebook Employee Monitoring

For monitoring ChromeOS or Chromebook devices, you can use Cloud connection and/or Reverse Connection. If you want to use Cloud connection, make sure that you already created the Cloud account as described in the Cloud installation section.

Console Configuration — Reverse Connection Server

To use Reverse Connection, enable Reverse Connection Server in the console. Use the menu Connection / Configure Console Reverse Connection Server. Set a Reverse Connection Server password. You may need to open port TCP 444 on the firewall of the console computer.



Screenshot: Configure Reverse Connection Server.

Installing the Chrome Extension on ChromeOS Device

Install the Chrome extension to monitor a ChromeOS device. The Chrome extension can be installed manually or deployed using Google Admin Console.

For manual installation, install the Net Monitor for Employees Pro Chrome extension on the ChromeOS device. Configure the Chrome extension by first selecting an Agent password that you can remember. If using Reverse Connection, configure the extension by setting the console IP and the Reverse Connection Server password specified in the previous step. The application also supports monitoring using multiple consoles; all computers must be on the same network. Use the + Add an additional Console to connect button to add multiple console computers. If using Cloud connection, configure the extension by setting your existing Cloud account and password.

chrome-extension://ibacgekigflemnhakpaamagjhgbclbjc/options.html

Net Monitor for Employees Options

Agent Configuration

Client Name:
EMPLOYEE.NAME

Unique Computer Id (e.g. MAC Address):
ac8ad65c2ed0a98787cacd73b72879ef

Agent Password:

Confirm Agent Password:

Connection Type:

☒ Use Cloud connection (connect via the Internet)

☐ Use reverse connection - console acts as a server (connect via local network - LAN/WLAN)

Cloud Configuration

Cloud Account:
my_cloud_account

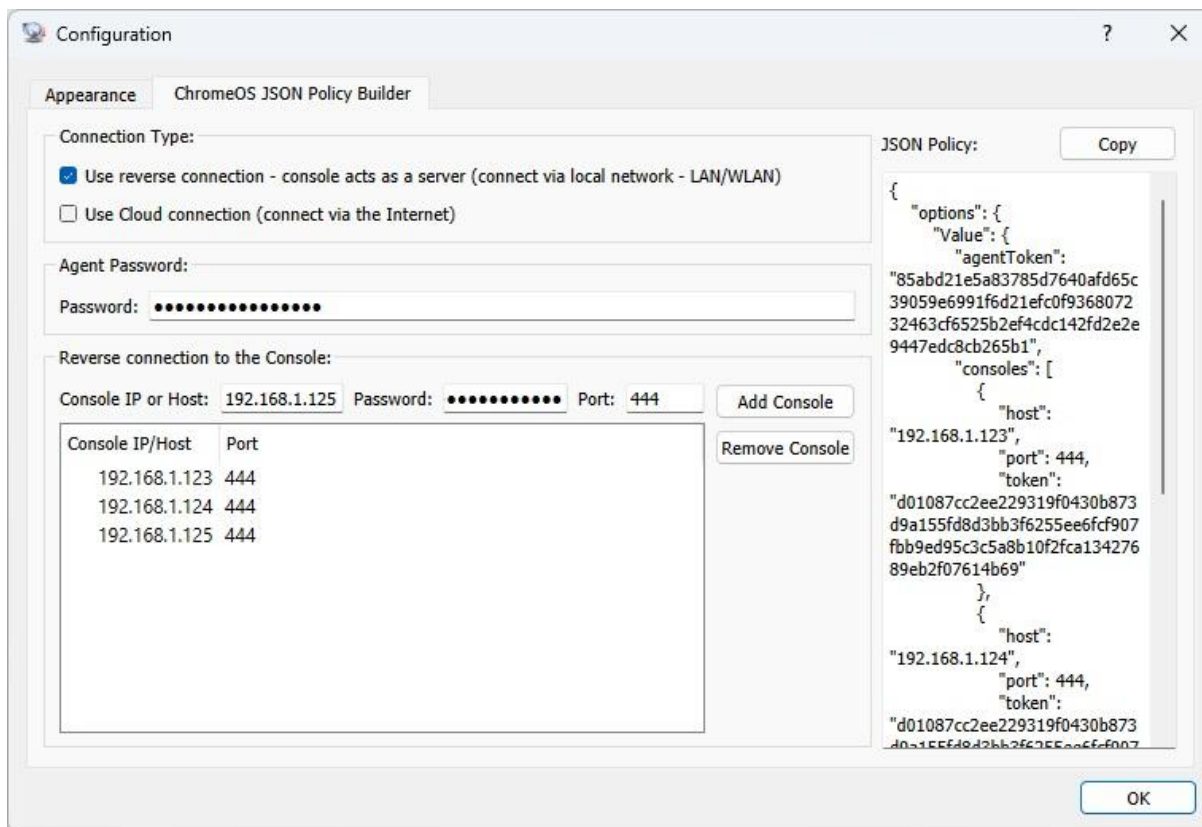
Cloud Account Password:

Save configuration

Screenshot: Chrome extension configuration.

Chrome Extension Deployment Using Google Admin Console

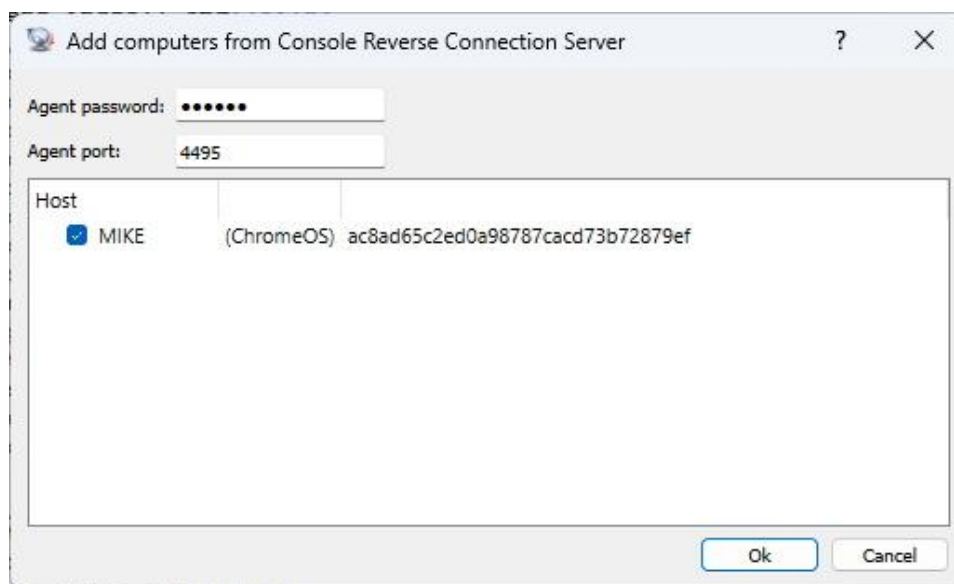
The Chrome extension can also be deployed using Google Admin Console. In this case, prepare a JSON Policy for deployment. Use the console menu File / Configuration to generate JSON Policy based on your configuration data. In Reverse Connection mode, the Chrome extension connects to the console. For this reason, you can monitor ChromeOS devices only when they are on the same network as the console. Chromebook must be running and have direct network access to the console.



Screenshot: Generate JSON policy for Chrome extension deployment.

Add ChromeOS Device to the Console

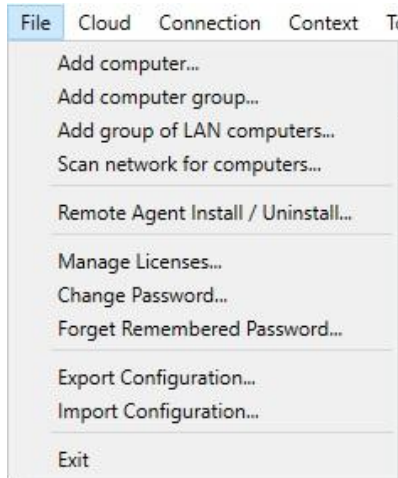
If using Reverse Connection, add the Chromebook using menu Connection / Add Computers from Console Reverse Connection Server. If using Cloud Connection, add Chromebook using menu Cloud / Add Computers from Cloud.



Screenshot: Add computers from Reverse Connection Server.

3. Using the Monitoring Console

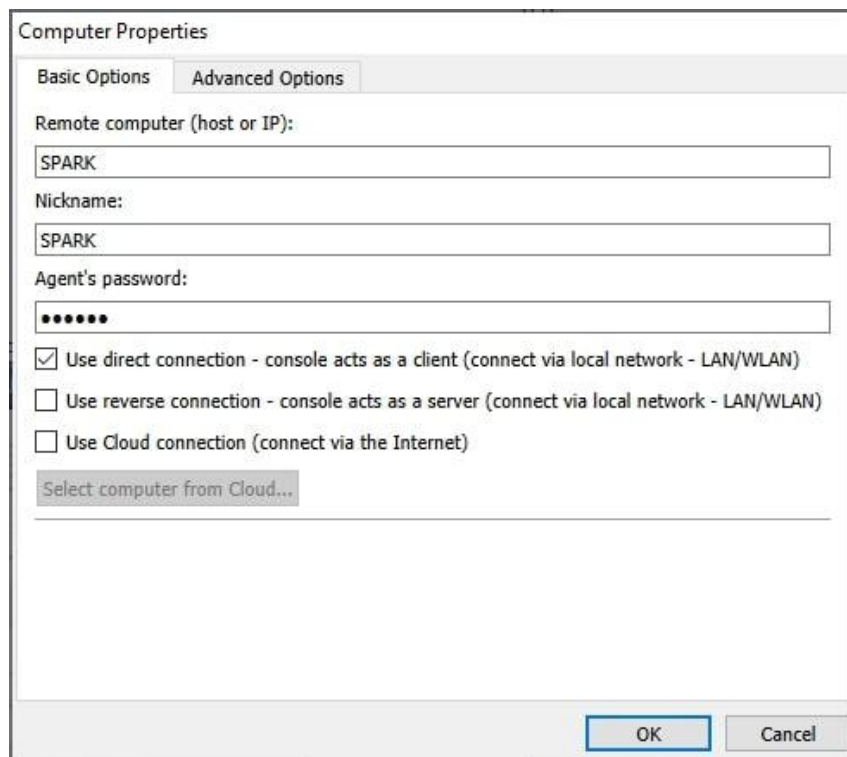
To monitor remote computers, first add them to the console. You can add computers manually, add computers from Cloud, scan network for installed agents, or add a group of LAN computers.



Screenshot: File menu options for adding computers.

3.1 Add Computers Manually

Select Add computer... from the File menu. The dialog has two tabs: Basic Options and Advanced Options.



Screenshot: Add computer — Basic Options.

Basic option	Description
Remote computer (host or IP)	Enter the network hostname or IP of the remote computer. When using DHCP on the local network, enter the computer name.
Nickname	Enter the name that you want displayed to easily identify the remote computer.
Agent password	Enter the same password used when installing the agent.
Connection Type — Direct Connection	A direct TCP/IP connection between console and agents. The console acts as client, the agent as server. Default TCP 4495 must be enabled.
Connection Type — Reverse Connection	The console acts as server and the agent as client. Enable Console Reverse Connection Server and specify console host name or IP. Default TCP 444 must be enabled.
Connection Type — Cloud Connection	Makes the computer accessible through Cloud connection for monitoring over the Internet. Cloud license is subscription based.

Computer Properties

Basic Options Advanced Options

TCP Port:
4495

☒ Connect automatically

Monitor: (all monitors) ▼

☐ Show camera of this remote computer

Warning:
The camera light will turn on if you enable the camera view.
When a camera is enabled then other applications (e.g. video conferencing apps) will not be able to use the camera.
If some application is currently using the camera then you will not be able to see the video stream from the camera.

Multisession - terminal (TS, RDP) options

☒ Automatic selection

☐ This computer supports only one session

☐ This computer is a terminal server (TS, RDP)

OK Cancel

Screenshot: Add computer — Advanced Options.

Advanced option	Description
TCP Port	Enter the same port used when installing the agent. The default port is 4495.
Connection security	Choose Auto (tries TLS first, falls back to end-to-end encryption only if the agent doesn't answer with TLS at all), or force End-to-end encryption or TLS to match the agent's own setting. When TLS is used, the console remembers ("pins") the certificate's fingerprint the first time it connects and checks it on every later connection; a Forget button clears a pinned fingerprint (for example after reinstalling an agent with a new certificate). If the console is set to hold new certificates for approval instead of trusting them automatically (see Configuration / General), a certificate awaiting

	approval is shown here too, with a Trust... button to review its fingerprint and confirm it.
Connect automatically	Mark this checkbox if the remote computer should be automatically connected when the console starts.
Monitor	Select which monitor will be displayed as thumbnail.
Multisession — terminal (TS, RDP) options	Select if your computer is an RDP/TS server. This allows you to see all remote sessions.

Account filter

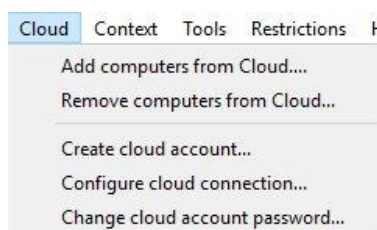
Use the Account filter tab in Computer Properties to choose which Windows user accounts on a computer are monitored.

Choose “Monitor all accounts except selected” to monitor every account except the ones you list (for example, exclude Administrator), or “Monitor only selected accounts” to monitor only the accounts you list.

The filter is applied per session, so it also works correctly when the computer is a terminal server (TS, RDP) with several users logged in at the same time – each session's account is checked independently, and non-monitored accounts simply don't appear in the console.

3.2 Add Computers from Cloud

If you installed the agent on remote computers using Cloud Connection, you can add those computers to the console. Make sure that you created a Cloud account. Cloud account can be created during agent installation or by using menu Cloud / Create cloud account.



Screenshot: Configure Cloud Monitoring menu.

Note:
Using a Cloud connection allows you to monitor your users over the Internet and not only on your local network. This option is charged as a subscription and requires a Cloud account.

☒ Enable cloud connection

Enter your existing cloud account here:

Account name: my_cloud_account

Password:

Status: Connected

Forgot account password? Enter your email or account name to reset the password.

E-mail:

Account name:

Reset Password...

Don't have the cloud account yet? Create it now.

Create Cloud Account...

Ok Cancel

Screenshot: Cloud connection configuration in the console.

If you already created a Cloud account, enter this Cloud account login information in the console using menu Cloud / Configure cloud connection. After that, use menu Cloud / Add computers from Cloud to add computers already added to the Cloud. When adding computers from the Cloud, enter the agent password that was used during agent installation on the remote computer.

3.3 Scan Network for Installed Agents

IP range and agent data

Network adapter: Ethernet (192.0.2.10)

From (IP): 192 . 0 . 2 . 1

To (IP): 192 . 0 . 2 . 254

Agent password:

Agent port: 4495

Scan

Discovered computers

☐ Show only computers not yet added

Hostname	IP	State	OS	Agent version
☒ COMPUTER-01	192.0.2.21	Password ok	Windows 11	6.5.3
☒ COMPUTER-02	192.0.2.22	Password ok	macOS 15.5	6.5.3
☒ COMPUTER-03	192.0.2.23	Password ok	Ubuntu 24.04 LTS	6.5.3
☐ COMPUTER-04	192.0.2.24	Wrong password!		

Select all Unselect all

☐ Add computers using IP instead of computer name (not recommended on DHCP)

Add Close

Screenshot: Scan network for installed agents.

If you already installed agents on remote computers, scan the network and add them automatically.

Scanning does not require choosing a connection type in advance - it tries TLS first for every address and falls back to end-to-end encryption only when an address actively answers but rejects TLS, so agents using either mode are found without extra configuration.

Choose the network adapter and IPv4 range, enter the agent password and port, then click **Scan**. Click **Stop** to stop an active scan.

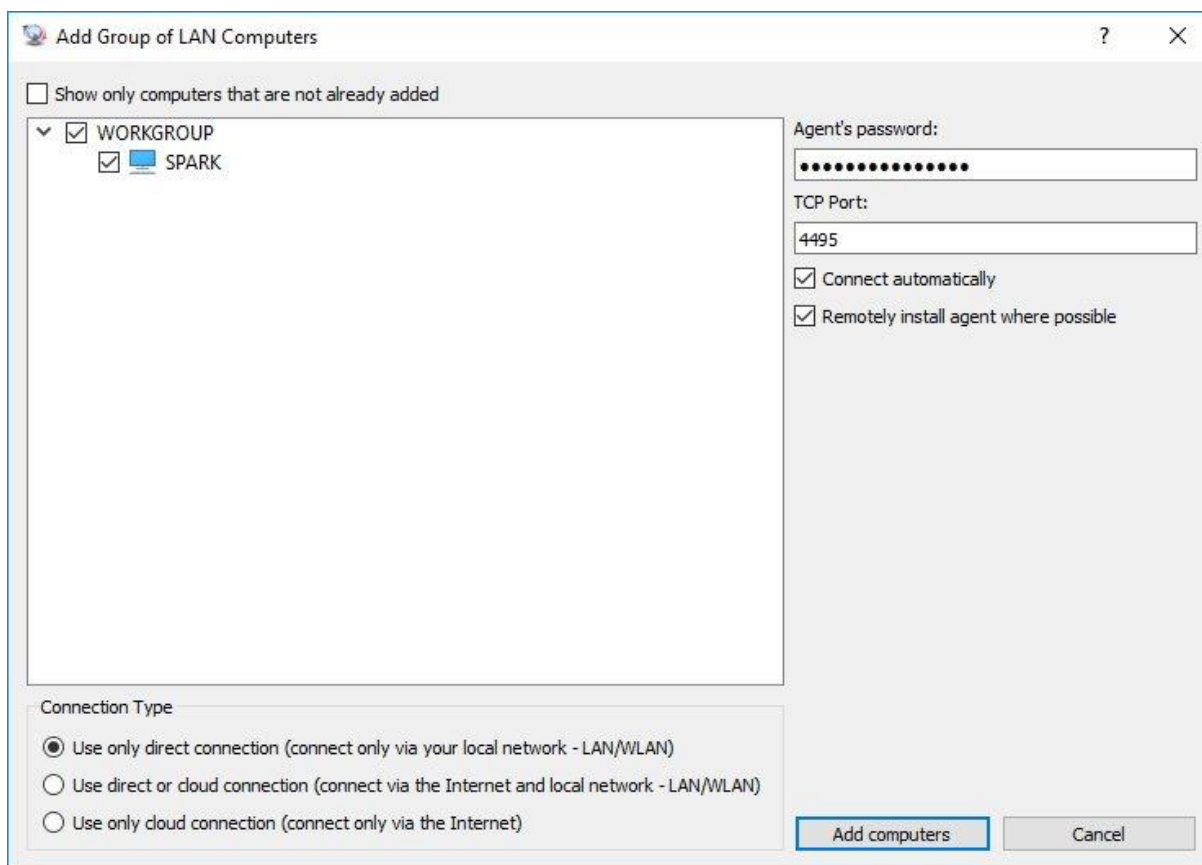
The results show the hostname, IP address and password status. When the password is correct, **OS** shows the reported operating system with its icon, and **Agent version** shows the reported agent version. These details appear only when available; there is no separate OS version column or unknown-value placeholder.

Show only computers not yet added is unchecked by default, so all discovered computers are shown. Check it to hide computers whose hostname or IP address is already in the console. Clear it to show them again.

Use **Select all** or **Unselect all** to change the checkboxes for the currently visible results. Individual choices are preserved as more results arrive and when the filter changes. **Add** adds only checked, visible computers. Columns automatically fit their widest entry.

In computer **Properties**, the OS icon sits immediately to the left of the reported operating system name; the agent version is shown when available. If an older agent reports Windows 10 on a Windows 11 computer, update the agent and reconnect or scan again.

3.4 Add Group of LAN Computers

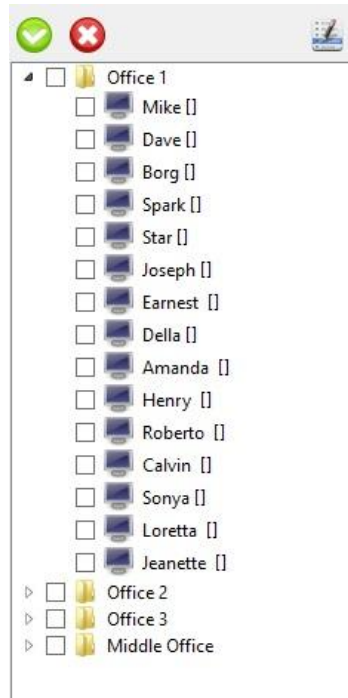


Screenshot: Add a group of LAN computers.

You can automatically add computers on your LAN. The agent can be installed remotely if your LAN permits this, for example if you are an NT Domain Administrator.

The **Show only computers not yet added** checkbox is also available in **Add group of LAN computers**. It is unchecked by default; check it to hide computer names already added to the console.

3.5 Remote Computers List



Screenshot: Remote Computers List / computer tree.

The Remote Computers List displays all computers added. The computer icon displays the state of the remote computer. Several system commands can be accessed using the Object Menu, invoked with a right mouse click. Computers can be organized in groups using Add computer group... from the File menu.

Right-click a computer group and select “Filter by this group on Remote Screens” from the Object Menu to instantly filter the Remote Screens tab to that group – the same filter you can also set using the group filter drop-down on the Remote Screens tab.

By default, all computer groups are expanded when the console starts. This can be changed using Configuration... from the File menu, General tab, by unchecking “Expand groups when console starts”.

The same General tab has "Automatically trust a computer's certificate the first time it connects over TLS", checked by default. Uncheck it to hold a new computer's certificate for your approval instead of trusting it automatically - see Connection security above.

3.6 Import and Export Computers (CSV, Tab-Delimited, Excel)

Computers and groups can be bulk-exported to a CSV, tab-delimited text, or Microsoft Excel (.xlsx) file, and imported back. Choose “Export Computers to File...” and “Import Computers from File...” from the File menu, or right-click a computer group (or an empty area of the list to include everything) and choose the same commands from the Object Menu. Files are read and written as UTF-8.

When exporting, pick the file type directly in the Save dialog: CSV (Comma delimited), CSV (Semicolon delimited), Tab Delimited Text, or Microsoft Excel. On import, the delimiter of a CSV or tab-delimited file is detected automatically.

The exported file uses the column order below. Columns can be reordered on import as long as the header row keeps the same column names; unrecognized columns are ignored, and a column left empty uses the default shown below — only host is required:

Column	Description	Default when empty
group	Group path of the computer, e.g. /Lab1/RoomA. Missing groups are created automatically on import.	Root (/)
name	Display name (nickname) shown in the console.	Falls back to host
host	IP address or hostname of the remote computer.	Required — row is skipped if empty
port	Agent connection port.	Default agent port
password	Agent connection password.	See note below — never exported
connection_type	Direct, Reverse, Cloud, or a comma-separated combination.	Direct
auto_connect	Yes or No — whether the console connects automatically at startup.	Yes
multisession	Automatic, Single, or Multi.	Automatic
hwid	Hardware ID of the agent’s Cloud registration.	Required to auto-connect a Cloud entry; see note below

The password column is always left empty on export — passwords are never written to the file. On import, a common password can be entered once and is used for every row whose password column is empty; a row with its own password value uses that value instead.

For a computer whose connection_type includes Cloud, hwid should also be provided — it identifies the agent’s Cloud registration. If it is left empty, open the imported computer’s Properties and re-enable Use Cloud connection to select the matching computer from your Cloud account and reconnect it.

4. Live Monitoring and Remote Screens

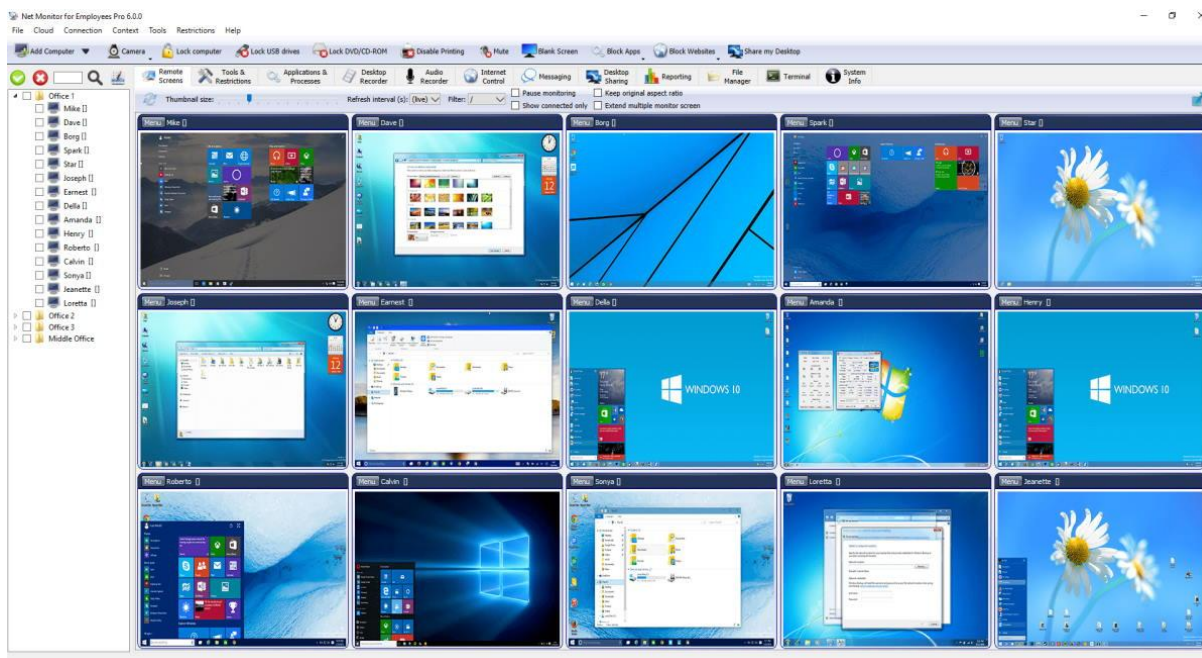
Remote Screens can be used for live supervision of many remote computers at once without interrupting employees. This feature allows managers to quickly notice unusual behavior and focus only on remote computers that need attention.

Typical Use Cases

- Watching employee screens live during normal work shifts.
- Checking if employees are using required work applications.
- Spotting non-work activity early and reacting quickly.
- Following remote employees during work-from-home hours.
- Verifying that restrictions and admin actions were applied correctly.

Remote Screens Overview

The Remote Screens tab displays live thumbnails of all selected remote computers. It is the main real-time monitoring workspace.



Screenshot: Remote Screens tab with multiple live thumbnails.

Toolbar Controls

- Refresh: request a new frame immediately.
- Thumbnail size: tune layout density versus detail.

- Refresh interval: use live for highest fidelity or a larger interval to reduce traffic.
- Filter: show only the selected group.
- Keep original aspect ratio: avoids stretched thumbnails.
- Show connected only: hides disconnected computers.
- Extend multiple monitor screen: shows multi-monitor desktop as one extended area.
- Pause monitoring: temporarily freezes updates.
- Full screen: expands monitoring workspace.

Camera Tiles

If remote computers have available cameras, camera tiles can be shown near desktop thumbnails. Visibility can be switched globally to show configured cameras, show all, or hide all.

Recommended Workflow

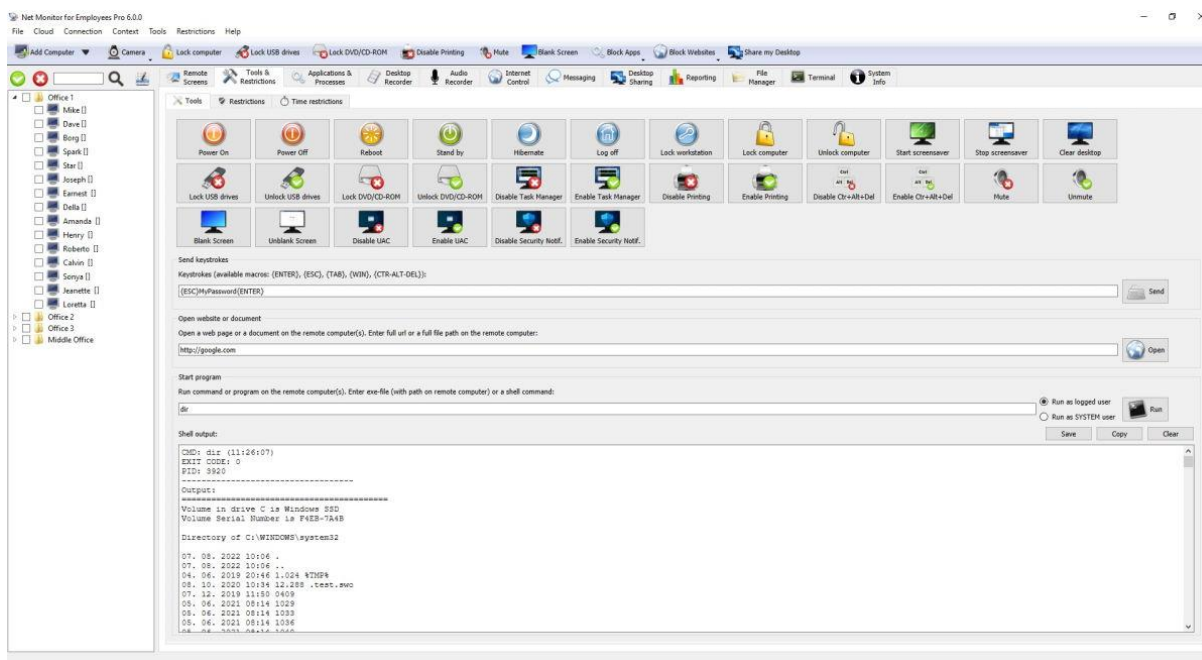
7. Select computers or groups in the tree.
8. Set refresh interval and thumbnail size for current network conditions.
9. Enable connected-only view in large environments.
10. Use right-click Object Menu from a thumbnail for quick actions such as Remote Control.

5. Control Tools and Restrictions

Tools and Restrictions can be used to run immediate actions on employee computers and apply rules that stay active. This feature allows managers to react fast during incidents, enforce work policy, and keep employee computer use under control.

- Showing an urgent message on all selected computers during an incident.
- Locking USB, printing, or Task Manager during exams, audits, or sensitive projects.
- Setting daily time limits so employees log off after allowed usage time.
- Quickly restarting or locking selected computers when policy is violated.
- Applying temporary controls while managers investigate suspicious activity.
- Restoring normal access after the monitoring or incident action is finished.

5.1 Tools Tab — Immediate Actions



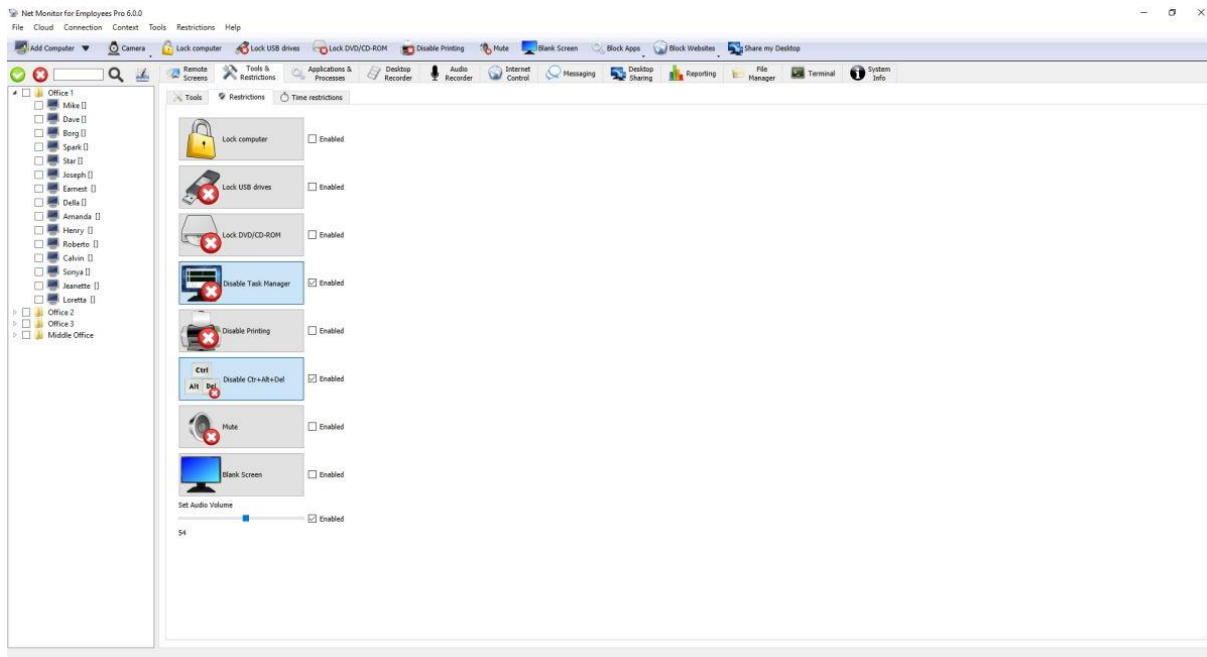
Screenshot: Tools tab with immediate computer actions.

This tab executes actions immediately on selected computers. The console executes actions directly on selected employee computers.

Action	What it does
Power On	Turns on selected computers (Wake-on-LAN, if available).
Power Off	Shuts down and powers off the computer.
Reboot	Restarts the computer.
Stand by	Puts the computer to sleep.
Hibernate	Saves current work and powers down.
Log off	Signs out the current user.
Lock workstation	Locks the current user session.
Lock computer	Blocks keyboard and mouse use until admin unlocks it.
Unlock computer	Removes the lock set by Lock computer.
Start screensaver	Starts the screensaver on the remote computer.

Stop screensaver	Stops the screensaver on the remote computer.
Clear desktop	Clears desktop items from view (depends on OS support).
Lock USB drives	Blocks USB storage use.
Unlock USB drives	Allows USB storage use again.
Lock DVD/CD-ROM	Blocks DVD/CD drive use.
Unlock DVD/CD-ROM	Allows DVD/CD drive use again.
Disable Task Manager	Stops users from opening Task Manager.
Enable Task Manager	Allows Task Manager again.
Disable Printing	Stops printing.
Enable Printing	Allows printing again.
Disable Ctrl+Alt+Del	Turns off Ctrl+Alt+Del options on supported systems.
Enable Ctrl+Alt+Del	Turns Ctrl+Alt+Del options back on.
Mute	Mutes system sound.
Unmute	Unmutes system sound.
Blank Screen	Shows a blank screen to the user.
Unblank Screen	Shows the normal screen again.
Disable UAC	Turns off UAC prompts on supported Windows computers.
Enable UAC	Turns UAC prompts back on.
Disable Security Notifications	Turns off security notifications on supported Windows computers.
Enable Security Notifications	Turns security notifications back on.
Additional command	What it does
Send Keystrokes	Sends keyboard input to selected computers. Supported macros are {ESC}, {TAB}, {ENTER}, {WIN}, {CTR}, {CTR-ALT-DEL}, {BACKSPACE}, {INSERT}, {DELETE}, {HOME}, {END}, {PGUP}, {PGDN}, {LEFT}, {UP}, {RIGHT}, {DOWN}, and {F1} to {F12}. {CTR-ALT-DEL} sends the real secure key combination.
Open Website or Document	Opens a website URL or document path on selected computers.
Start Program	Runs a command on selected computers as logged user or SYSTEM and shows command output.

5.2 Restrictions Tab — Persistent Restrictions



Screenshot: Restrictions tab for persistent employee computer restrictions.

Use this tab for restrictions that stay active. Unlike Tools, these settings are applied globally to all employee computers, not only currently selected computers.

Restriction	What it does when enabled
Lock computer	Keeps keyboard and mouse blocked until you disable this restriction.
Lock USB drives	Keeps USB storage blocked.
Lock DVD/CD-ROM	Keeps DVD/CD drive use blocked.
Disable Task Manager	Keeps Task Manager disabled.
Disable Printing	Keeps printing disabled.
Disable Ctrl+Alt+Del	Keeps Ctrl+Alt+Del options disabled on supported systems.
Mute	Keeps sound muted.
Blank Screen	Keeps screen blank.
Set Audio Volume	Keeps a fixed sound level.

When you enable a restriction, the action is applied right away. When you disable it, the reverse action is sent, for example lock USB / unlock USB. Settings are stored on the remote computer and applied again after reconnect.

5.3 Time Restrictions Tab — Daily Computer Time Limits

This tab is based on daily active usage minutes per user. The agent checks usage regularly. When the daily limit is reached, it runs the selected action. If Show message is enabled, users first see your message, then the action runs. Restrict Administrator accounts decides if admin sessions are also limited.

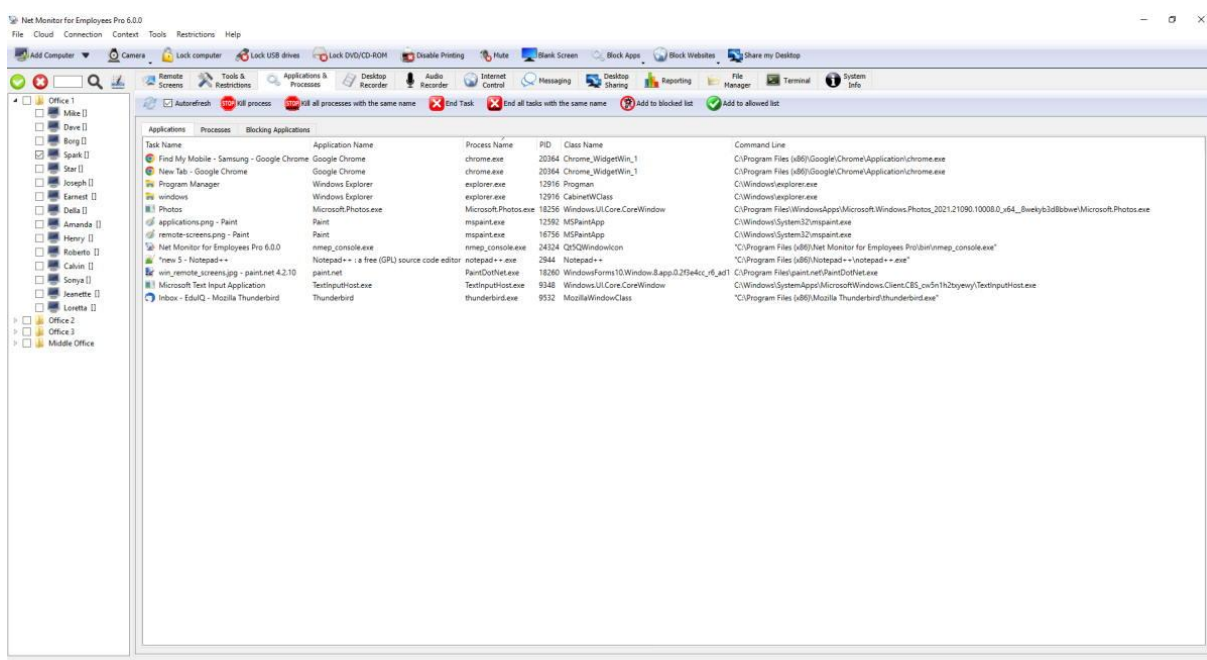
Action	What happens after the configured daily usage threshold
Power Off	Shuts down the computer.
Reboot	Restarts the computer.
Stand by	Puts the computer to sleep.
Hibernate	Puts the computer into hibernation.
Log off	Signs out the current user.
Lock workstation	Locks the current user session.

6. Applications and Process Restrictions

Applications and Processes can be used to discover and control running apps and background processes on remote computers. This feature allows managers to quickly stop unwanted apps and keep employees focused on approved work tools.

- Stopping unauthorized chat, game, or remote-access tools.
- Closing blocked applications on all selected computers.
- Ending stuck background processes that slow employee computers.
- Building an allow-only list for exam, kiosk, or focused-work mode.
- Checking which applications employees actually use during shifts.

Applications Tab

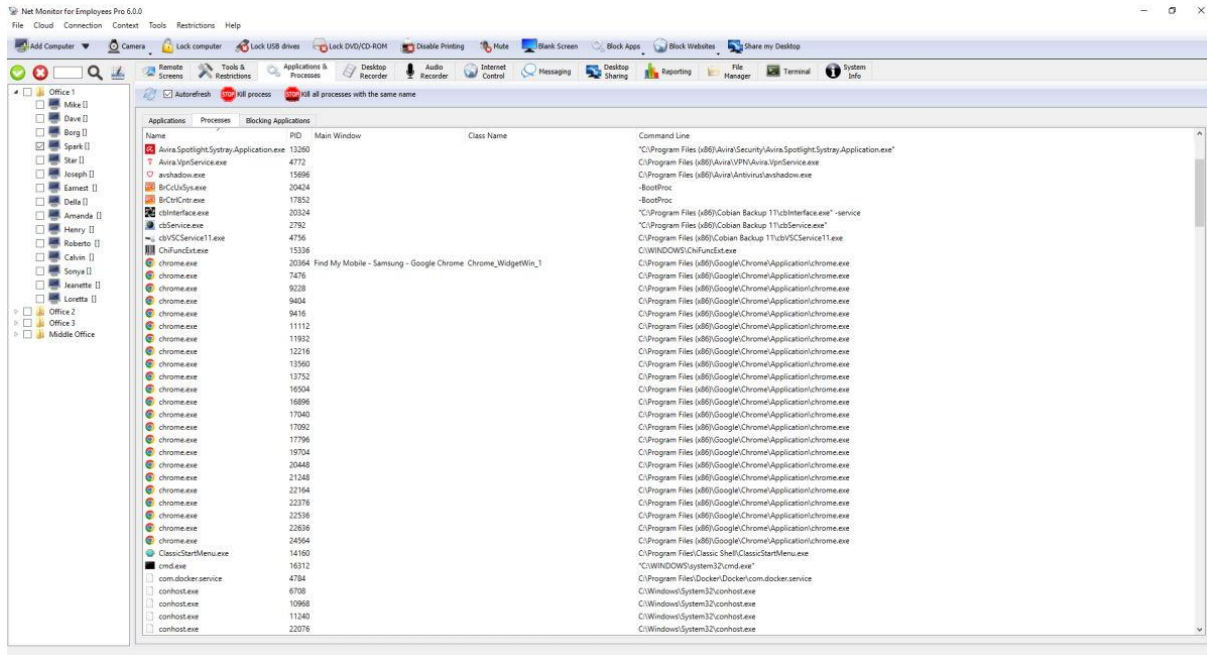


Screenshot: Applications tab showing visible applications.

This tab shows visible application windows and tasks. Use it when you need to act on user-facing apps.

- End Task closes the selected app on the current remote computer.
- End all tasks with same name closes the same app on all selected computers.
- Add to blocked/allowed list copies app names from selected rows into policy lists.

Processes Tab

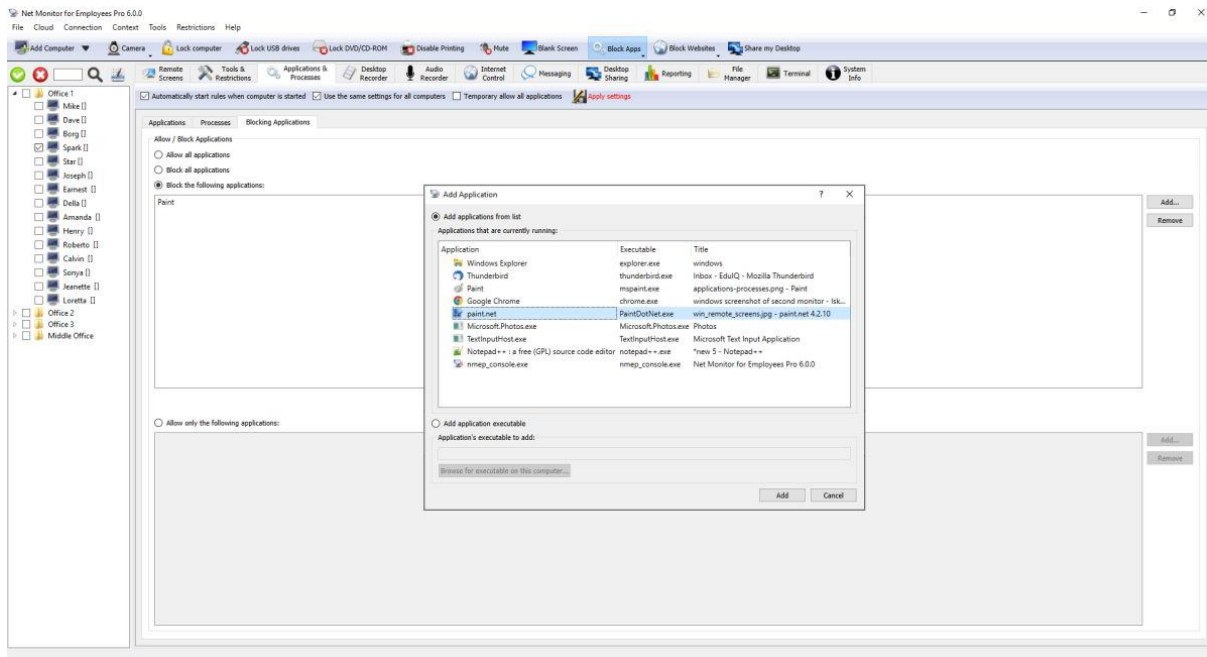


Screenshot: Processes tab with process-level controls.

This tab is process-level administration with PID, class, and command line. It is useful when applications have no visible task window.

- Kill process targets the selected PID on the current computer.
- Kill all processes with same name stops that process on all selected computers.
- Autorefresh runs every 5 seconds and keeps the list current while this context is active.

Blocking Applications Tab



Screenshot: Blocking Applications tab.

This tab defines remote computer run policy. The rule set is saved and sent as settings.

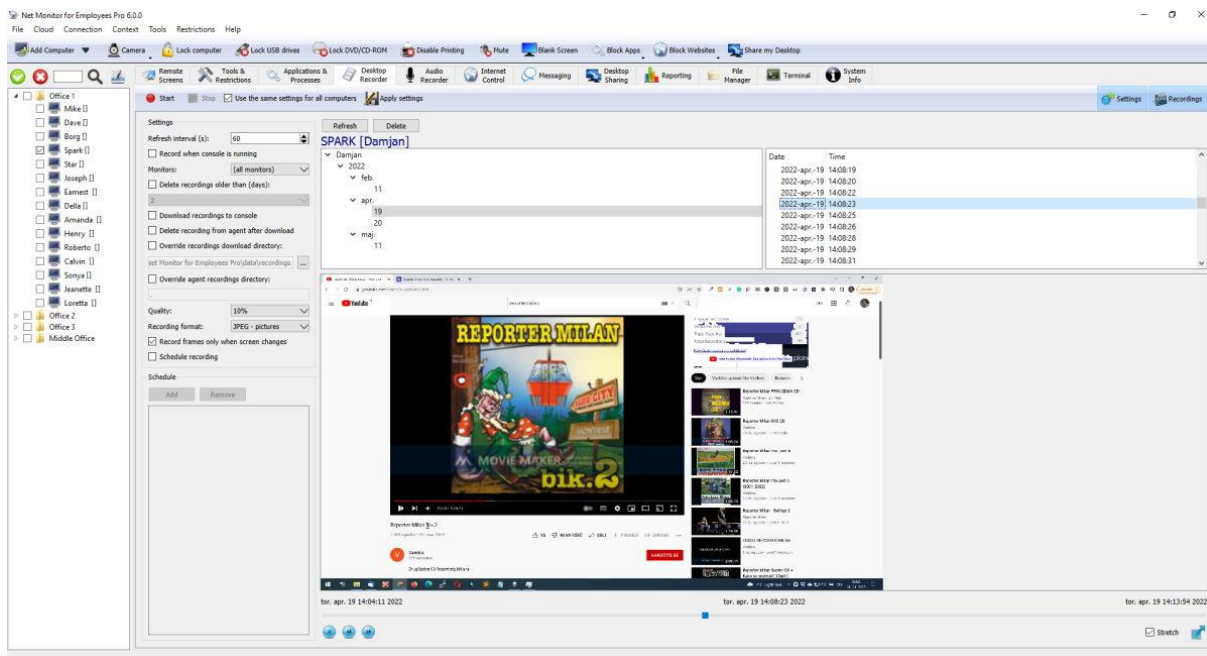
- Allow all, Block all, Block list, or Allow list.
- Automatically start rules starts automatic blocking when the remote computer starts.
- Use same settings for all computers keeps one shared policy and applies it globally.
- When shared settings is off, policy can be loaded per current computer and applied only to selected computers.
- Temporary allow all disables enforcement but keeps blocked/allowed lists intact.
- Apply settings applies current rule mode and list settings immediately.

7. Recording, Logging, and Reporting

7.1 Employee Screen Recording with Computer Screen Recorder

Desktop Recorder can be used to record employee screen activity on remote computers for later investigation. This feature allows managers to keep clear proof of what happened, even when they were not watching live.

- Checking what happened before a support issue or security incident.
- Keeping recordings of employee activity as proof for later use.
- Reviewing employee workflow and discussing improvements during follow-up meetings.
- Coaching new employees using real examples from past recordings.
- Confirming repeated policy violations with visual evidence.



Screenshot: Desktop Recorder configuration and recordings browser.

Desktop Recorder captures remote screens as JPEG snapshots or MKV/MPEG4 video files. You can run it manually, by schedule, or tied to console connection status.

Top Toolbar

- Start applies current settings first, then starts recording on selected computers after confirmation.
- Stop stops recording on selected computers after confirmation.
- Use the same settings for all computers controls scope: enabled means one profile for all computers, disabled means selected computers only.
- Apply settings sends configuration changes without forcing Start/Stop. If settings were changed and not applied yet, Apply settings blinks red.
- Settings and Recordings buttons show/hide left configuration panel and right recordings panel.

Left Settings Panel

- Refresh interval (s): capture period. Lower values increase detail and storage usage. Recorder captures at about one frame per second minimum.
- Record when console is running: starts when console connects and stops when console disconnects unless schedule is active.
- Monitors: select primary monitor, all monitors, or a specific monitor index.
- Delete recordings older than (days): automatic retention cleanup.
- Download recordings to console: enables automatic background download from agents.
- Delete recording from agent after download: removes remote file after successful transfer.
- Override recordings download directory: custom local archive path. If disabled, default console recordings folder is used.
- Override agent recordings directory: custom recording path on monitored computer.
- Quality: 0% to 100% compression quality.
- Recording format: JPEG sequence, MKV video, or MPEG4 video.
- Max file size (Mb): available for video formats only. When limit is reached, recorder starts a new file. “Don’t limit” means unlimited.
- Record frames only when screen changes: skips duplicate frames and reduces storage/network usage.
- Schedule recording: enables schedule rules below. Use Add/Remove to create entries by weekday and all-day or time interval.

Recordings Browser and Player

- Refresh reloads filters and recording list.
- Delete removes selected recordings from agent and local downloaded archive.
- Filter tree groups recordings by User → Year → Month → Day.
- Recording list shows Date/Time; selecting an item positions playback to that recording.
- Player timeline spans all recordings in selected filter, not just one file.
- Player controls: Play/Pause, Previous, Next, Stretch, and Full Screen.
- Downloaded local files are merged with remote files in one list so playback works online and offline.

How Download Works

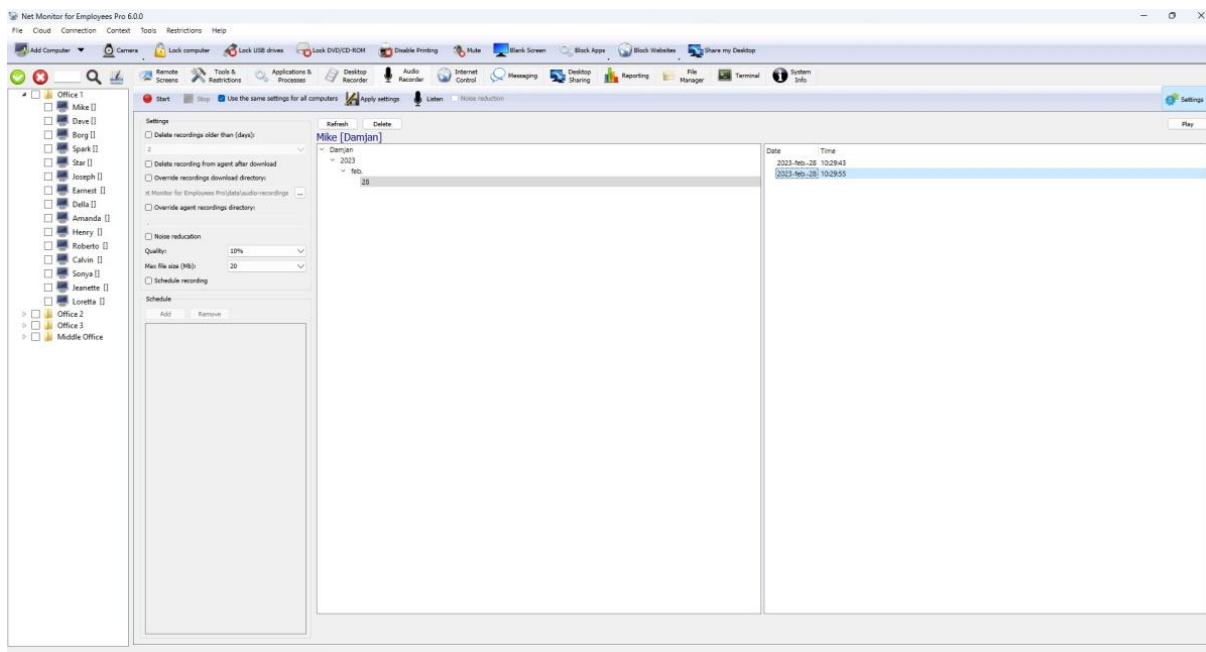
When download is enabled, the console periodically checks connected agents, queues missing files per host, downloads through a temporary local folder, and then moves completed files into the final archive path. Optional delete-after-download is applied after successful transfer.

Recommended setup: For long-term low-storage recording, use JPEG + screen-change detection + a longer interval.

7.2 Employee Audio Monitoring with Computer Audio Recorder

Audio Recorder can be used to capture remote computer microphone and speaker audio and to listen live when needed. This feature allows managers to hear call and meeting context when screen activity alone is not enough.

- Checking if employees follow required call scripts.
- Investigating complaints where spoken conversation matters.
- Keeping audio proof from incidents for later review.
- Running scheduled recording during high-risk time periods.



Screenshot: Audio Recorder screen.

Audio Recorder captures remote computer microphone/speaker audio, supports scheduled recording, and includes live listen mode for immediate supervision.

Toolbar Actions

- Start and Stop control recording on selected computers.
- Apply settings saves and sends the current profile to remote computers.
- Use the same settings for all computers switches between shared policy and per-computer profile.
- Listen starts/stops live audio streaming with source and noise-reduction options.

Recording Settings Explained

- Record microphone and Record speaker choose capture sources.
- Noise reduction improves clarity on noisy remote computers.
- Quality controls compression level.
- Max file size (Mb) rolls to a new file when threshold is reached.
- Schedule recording uses schedule tasks to start/stop automatically.

Storage and Download Pipeline

- Recordings are saved as .ogg audio files.
- Console downloads recordings in background and merges local and remote lists in one browser.
- Downloads use a bounded background queue so transfers remain responsive when many computers are connected.
- Delete recording from agent after download keeps remote computer storage low.
- Override download location lets you choose where downloaded audio files are stored.

Recordings Browser

- Left tree filters by user/date; right list shows recording timestamps.

- List supports playback and file actions for selected records.

7.3 Recording External Storage

Desktop and audio recordings can remain on each monitored computer and optionally be downloaded to the console, or each agent can upload them directly to a configured external storage profile.

Configure and Assign a Storage Profile

- Open File / Configuration / Recording External Storage.
- Click New, select a provider, enter a unique profile name and credentials, and specify an optional Folder.
- For SFTP, use Get key... to retrieve the SSH server host key, review it, and confirm it. Omitting the key disables server identity verification and displays a warning.
- Use Test connection to verify folder creation, upload, listing, download, deletion, and cleanup. The test runs in the background.
- Click Save to store profile changes, or Undo to discard unsaved changes.
- In Desktop Recorder or Audio Recorder, choose the named profile under Recording storage and click Apply settings for the selected agents.

Multiple profiles are supported, including multiple profiles of the same provider type. Credentials are stored in encrypted application configuration and are not written to logs.

Supported Providers and Security

SMB 2/3, SMB 1.0, FTP, WebDAV, SFTP, Amazon S3 and compatible S3 services, Google Cloud Storage, and Azure Blob Storage are supported.

Warning: SMB 1.0 and FTP are unsafe legacy protocols. FTP sends credentials and recordings without encryption. Prefer SMB 2/3, SFTP, WebDAV over HTTPS, or an HTTPS object-storage endpoint.

Provider Configuration Steps

The following steps explain every field shown in the storage profile and where to obtain its value.

SMB 2/3

- On the NAS or file server, create a share and a dedicated account with permission to list, create, read, write, and delete files and directories.
- SMB server: enter the DNS name or IP address without \\ or a share name.
- Share: enter only the share name.
- User name and Password: use the dedicated credentials supplied by the NAS or server administrator.
- Domain: enter the Active Directory/NT domain for a domain account; leave it empty for a local server or NAS account.
- Folder: optionally enter a relative folder below the share.

Using a Windows Shared Folder

- Create a folder such as D:\Recordings and a dedicated local or domain Windows account with a strong password. Do not use guest access.
- Open folder Properties / Sharing / Advanced Sharing, select Share this folder, and enter a share name such as Recordings.

- Under Sharing / Permissions, add the dedicated account and allow Change and Read. Remove broad access that is not required.
- On the Security tab, add the same account and allow Modify. Both share and NTFS permissions must allow access.
- On a trusted network, use the Private network profile and enable Network discovery and File and printer sharing under Settings / Network & internet / Advanced network settings / Advanced sharing settings.
- Enable the Windows Firewall File and Printer Sharing (SMB-In) rule for the trusted profile. Agents must reach TCP port 445.
- In the profile, enter the Windows computer name or IP as SMB server and the Advanced Sharing name as Share.
- For Active Directory, enter the AD domain. For a local account, normally leave Domain empty; if qualification is required, use the Windows computer name as the domain.
- Run Test connection. If it fails, verify both permission sets and test \\server\share from another computer with the same account.
- Use SMB 2/3 for modern Windows. Do not install or enable SMB 1.0.

SMB 1.0

- WARNING: SMB 1.0 is obsolete and unsafe. Use it only with an isolated legacy server that cannot support SMB 2/3.
- Fill the same server, share, credentials, domain, folder, and permissions as SMB 2/3. SMB 1.0 must already be enabled on the server.

FTP

- WARNING: FTP sends credentials and recordings without encryption. Prefer SFTP or WebDAV over HTTPS.
- Ask the server or hosting administrator for an FTP account with list, create-directory, upload, download, and delete permission.
- FTP server: enter a DNS name or IP address. An ftp:// URL is also accepted. Port: keep the default port 21 or enter the port supplied by the FTP administrator.
- User name and Password: enter the credentials from the server or hosting control panel.
- Folder: optionally enter a folder below the login directory. Start with / for an absolute path when the server permits it. The firewall must allow passive FTP data connections.

WebDAV

- Obtain an account and the URL of an existing WebDAV collection from the provider or server administrator. A typical Nextcloud URL is https://server.example.com/remote.php/dav/files/user.
- WebDAV URL: enter the full HTTPS collection URL.
- User name and Password: enter the WebDAV credentials. Use an application password when multifactor authentication is enabled and the provider supports one.
- Folder: optionally enter a folder below the collection URL.
- The account must permit PROPFIND, MKCOL, PUT, GET, and DELETE. The base collection must already exist.

SFTP

- Ask the SSH/SFTP administrator for the server, port, account, writable folder, and allowed authentication method. The server must allow SFTP and either password or public-key authentication.
- SSH server: enter the DNS name or IP address. Port: keep the default port 22 or enter the port supplied by the SSH/SFTP administrator.
- Folder: enter a path relative to the login directory, such as recordings, or start with / for an allowed absolute POSIX path.

- User name: enter the SFTP account. For password authentication, leave Private key empty and enter Password. For public-key authentication, install the matching public key in `authorized_keys`, click Load..., and select an OpenSSH or PEM private key. Enter the private-key passphrase if the key is encrypted; otherwise leave it empty. Click Clear to return to password authentication.
- Click Get key..., compare the SHA-256 fingerprint with the server administrator's fingerprint, and confirm only when they match.
- The private-key contents, not the console-local file name, are saved in the storage profile for use by the agent. Protect the profile and use a dedicated passphrase-protected key where possible. The account needs list, create, read, write, and delete permission. The client private key authenticates the account; the separate server host key identifies the server. Omitting the host key disables server identity verification and is unsafe.

Amazon S3

Use a dedicated Amazon S3 general-purpose bucket and IAM user. Never use AWS root-account credentials or make the bucket public.

1. Sign in to the AWS Management Console with an administrator identity and open Amazon S3.
2. Select the AWS Region where recordings should be stored, for example eu-central-1.
3. Open Buckets / Create bucket and keep General purpose as the bucket type.
4. Enter a globally unique lowercase bucket name, for example organization-recordings-12345. Save the exact name.
5. Keep Object Ownership set to Bucket owner enforced and keep all Block Public Access options enabled.
6. For predictable quota cleanup, leave Bucket Versioning disabled. If versioning is required, add an S3 Lifecycle rule to expire noncurrent versions; otherwise deleted recordings can continue consuming storage. Default SSE-S3 encryption needs no extra permission. A customer-managed KMS key needs additional KMS permissions. Do not enable Object Lock if the application must delete recordings.
7. Create the bucket, then save its exact AWS Region code from the Properties page or bucket list.
8. Open IAM / Policies / Create policy, select the JSON editor, and paste this policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListRecordings",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::YOUR_BUCKET_NAME"
    },
    {
      "Sid": "ManageRecordings",
      "Effect": "Allow",
      "Action": ["s3:PutObject", "s3:GetObject", "s3:DeleteObject"],
      "Resource": "arn:aws:s3:::YOUR_BUCKET_NAME/*"
    }
  ]
}
```

9. Replace both occurrences of `YOUR_BUCKET_NAME` with the exact bucket name. Click Next, resolve validation errors, name the policy RecordingStorageS3, and create it.
10. Open IAM / Users / Create user. Enter recording-storage-agent and create the user without console access.

11. Open the user, select Permissions / Add permissions / Attach policies directly, select RecordingStorageS3, and add it.
12. Open Security credentials / Access keys / Create access key. Choose an application running outside AWS, or Other if shown, and create the key.
13. Copy the Access key ID and Secret access key, or download the CSV. AWS displays the secret only once.
14. In File / Configuration / Recording External Storage, create an S3-compatible storage profile. Leave HTTPS endpoint empty. Enter the exact Bucket, Region code, Access key ID, and Secret access key.
15. Folder is optional. Enter an object-key prefix such as recordings; do not include the bucket or computer name. The application creates the folder and computer/recording-type hierarchy automatically.
16. Save the profile and click Test connection. The test uploads, lists, downloads, and deletes temporary data.

Troubleshooting: AccessDenied (403) usually means the IAM policy is missing, not attached, or overridden by another policy. Wrong Region or AuthorizationHeaderMalformed means the Region code is incorrect. SignatureDoesNotMatch can indicate a mismatched key pair or incorrect computer clock. For KMS errors, use SSE-S3 or grant the required KMS-key permissions.

AWS references: <https://docs.aws.amazon.com/AmazonS3/latest/userguide/create-bucket-overview.html> ;
https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_create-console.html ;
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users_create.html ;
<https://docs.aws.amazon.com/IAM/latest/UserGuide/access-key-self-managed.html>

How to Use S3-Compatible Services

The following services use S3-compatible storage (including Amazon S3). Create the bucket and credentials in the provider portal first. Enter the HTTPS base endpoint without the bucket name, enter the name separately in Bucket, and optionally enter an object-key prefix in Folder.

The credentials must permit listing the bucket and creating, reading, and deleting objects. After completing each profile, click Save and Test connection. The service must support path-style bucket URLs, AWS Signature Version 4, and S3-compatible XML listing responses.

How to Use Cloudflare R2 as External Storage

11. In the Cloudflare dashboard, open Storage & databases / R2 / Overview, click Create bucket, and save the exact bucket name.
12. Open Manage R2 API Tokens, create an Account API token, grant Object Read & Write, and restrict it to the recording bucket.
13. Copy the Access Key ID, Secret Access Key, and S3 endpoint while they are displayed.
14. Create an S3-compatible profile. Set HTTPS endpoint to https://<ACCOUNT_ID>.r2.cloudflarestorage.com, Bucket to the exact name, Region to auto, and enter the matching key pair. Optionally set Folder, then save and test.

Do not append the bucket name to the endpoint. Avoid retention rules that prevent application quota cleanup. Official guide: <https://developers.cloudflare.com/r2/get-started/s3/>

How to Use Backblaze B2 as External Storage

15. In the Backblaze console, open B2 Cloud Storage / Buckets, create a Private bucket, and save its name and region.
16. Open Application Keys / Add a New Application Key. Restrict the key to the bucket, enable Allow List All Bucket Names, and grant listFiles, readFiles, writeFiles, and deleteFiles.

17. Copy keyID and applicationKey. The application key is displayed only once; do not use the master application key.
18. Set HTTPS endpoint to <https://s3.<REGION>.backblazeb2.com>, Region to the same code (for example us-west-004), Access key to keyID, and Secret key to applicationKey. Enter Bucket and optional Folder, then save and test.

B2 retains old versions by default. Configure Lifecycle to remove hidden or previous versions when deletion must immediately release quota. Official guide: <https://www.backblaze.com/docs/cloud-storage-call-the-s3-compatible-api>

How to Use Wasabi as External Storage

19. In the Wasabi Console, open Buckets / Create Bucket, enter a unique name, and select the region nearest the agents. Keep the bucket private.
20. Leave Versioning and Object Lock disabled for predictable quota cleanup, or configure Lifecycle rules that remove retained versions.
21. Create a dedicated sub-user and bucket policy with list, get, put, and delete access, then use Access Keys / Create New Access Key and copy the key pair.
22. Use the regional service URL as HTTPS endpoint. For us-east-1 use <https://s3.wasabisys.com>. Set Region to the exact bucket region, then enter Bucket, optional Folder, Access Key, and Secret Key and test.

The endpoint and Region must match. Official service URLs: <https://docs.wasabi.com/docs/service-urls-for-wasabis-storage-regions>

How to Use DigitalOcean Spaces as External Storage

23. In the DigitalOcean Control Panel, open Spaces Object Storage / Create Bucket, choose the datacenter region, enter a unique Space name, and keep file listing restricted.
24. Choose Standard storage for recordings that will be listed and played regularly.
25. Create a dedicated Spaces access key, restrict it to the Space when available, and grant Read/Write/Delete. Copy the Access Key and Secret Key.
26. Set HTTPS endpoint to <https://<REGION>.digitaloceanspaces.com> (for example <https://nyc3.digitaloceanspaces.com>), Region to the same code, and Bucket to the Space name. Enter optional Folder and the keys, then save and test.

Use the origin endpoint, not a CDN or static-website endpoint. Official quickstart: <https://docs.digitalocean.com/products/spaces/getting-started/quickstart/>

How to Use MinIO as External Storage

27. In the MinIO Console, create a private bucket for recordings.
28. Create a dedicated user or service account and access key. Permit s3:ListBucket on `arn:aws:s3:::YOUR_BUCKET` and s3:GetObject, s3:PutObject, and s3:DeleteObject on `arn:aws:s3:::YOUR_BUCKET/*`.
29. Obtain the externally reachable S3 API URL and signing region from the administrator. The S3 API URL, such as <https://storage.example.com:9000>, is not necessarily the MinIO Console URL.
30. Enter the S3 API URL as HTTPS endpoint, the bucket name, optional Folder, and configured Region. Use us-east-1 only when the administrator confirms the default region. Enter the access-key pair, then save and test.

Every agent needs DNS and network access to the endpoint and must trust its HTTPS certificate. Official access guide: <https://docs.min.io/aistor/administration/console/security-and-access/>

How to Use Hetzner Object Storage as External Storage

31. In the Hetzner Cloud Console, select a project, open Object Storage, create a private bucket, and choose its location.
32. Save the location code: fsn1, nbg1, or hel1.
33. Open Security / S3 Credentials, click Generate credentials, enter a descriptive name, and securely copy the Access Key and one-time Secret Key.
34. Set HTTPS endpoint to <https://<LOCATION>.your-objectstorage.com>, Region to the same location code, and enter Bucket, optional Folder, and credentials. Save and test.

Use a bucket policy to restrict credentials shared with other applications. Official guide:

<https://docs.hetzner.com/storage/object-storage/getting-started/generating-s3-keys/>

How to Use IBM Cloud Object Storage as External Storage

35. In IBM Cloud, create or open a Cloud Object Storage service instance and create a private bucket. Save its exact name and location.
36. Open Service credentials / New credential, choose a role that permits listing, reading, writing, and deleting objects, such as Writer, and enable Include HMAC Credential.
37. Expand the new credential and copy `cos_hmac_keys.access_key_id` and `cos_hmac_keys.secret_access_key`. Do not use `apikey` in the S3 fields.
38. From the bucket Configuration page, copy the public S3 endpoint and signing location. Agents outside IBM Cloud normally require the public endpoint.
39. Enter the endpoint without the bucket name, the exact Bucket, optional Folder, and signing location in Region. For example, a US Standard cross-region bucket uses `us-standard`; do not infer Region only from the endpoint hostname.
40. Enter the HMAC access-key ID and secret, then save and test.

All agents must have routing and DNS access to the selected public, private, or direct endpoint. Official guide:

<https://cloud.ibm.com/docs/cloud-object-storage?topic=cloud-object-storage-service-credentials>

Google Cloud Storage

1. Prepare the project and bucket

- Sign in to Google Cloud Console and select or create a project with billing enabled.
- The administrator creating the HMAC key needs Storage HMAC Key Admin (roles/storage.hmacKeyAdmin). If key creation is unavailable, check organization policies that restrict authentication types or service-account key creation.
- Open Cloud Storage / Buckets / Create. Enter a globally unique bucket name and choose a location close to the monitored computers and suitable for your data-location requirements.
- Standard storage is a practical default for recordings that are uploaded, played, and deleted regularly. Use Uniform bucket-level access and keep public access prevention enabled.
- New buckets have seven-day soft delete by default. Disable it for predictable application quota cleanup or account for retained, billable deleted objects. Avoid retention locks when the application must delete old recordings.
- Keep Google-managed encryption unless your organization specifically requires customer-managed keys, then create the bucket.

2. Create and authorize the service account

- Open IAM & Admin / Service Accounts / Create service account. Use a descriptive name such as `recording-storage-agent` and finish without granting a project-wide storage role.

- Open the recording bucket's Permissions page, click Grant access, add the service-account email, and grant Storage Object User (roles/storage.objectUser) on this bucket only.
- Storage Object User supplies the required create, get, list, update, and delete object permissions without granting administration of other buckets.

3. Create the HMAC interoperability key

- Open Cloud Storage / Settings / Interoperability, click Create a key for a service account, and select the recording service account.
- Immediately copy both the HMAC Access ID and Secret; Google displays the secret only once. Allow up to 60 seconds for the new key to become usable.
- Do not create or download a JSON private key for this profile.

4. Configure and test the Google profile

- Create a Google Cloud Storage profile under File / Configuration / Recording External Storage.
- Leave HTTPS endpoint empty for <https://storage.googleapis.com>. Enter the exact Bucket, optionally enter a Folder, and keep Region set to auto.
- Enter the HMAC Access ID under Access key and its matching secret under Secret key. Set Recording quota manually or leave it unlimited, then click Save and Test connection.
- Troubleshooting: for 403 AccessDenied, check the bucket-level role and service-account email. InvalidAccessKeyId means the Access ID is wrong. SignatureDoesNotMatch usually means the secret or computer clock is wrong. For NoSuchBucket, verify the exact bucket name. If deleted data still occupies storage, check soft delete, Object Versioning, and retention policies.

Google references: <https://cloud.google.com/storage/docs/creating-buckets>, <https://cloud.google.com/iam/docs/service-accounts-create>, <https://cloud.google.com/storage/docs/access-control/iam-roles>, <https://cloud.google.com/storage/docs/authentication/managing-hmackeys>, and <https://cloud.google.com/storage/docs/soft-delete>.

Azure Blob Storage

Use a storage account dedicated to recordings when possible. This profile uses Shared Key; Microsoft Entra ID and SAS tokens are not accepted by these fields.

1. Create the storage account

- Sign in to Azure Portal, open Storage accounts / Create, and select a subscription and an existing or new resource group.
- Enter a globally unique 3-24 character name using lowercase letters and numbers. Select a nearby Region, Blob storage, Standard performance, and the redundancy required by your organization.
- Use the Hot access tier for recordings played regularly. Cool or colder tiers can add retrieval and minimum-retention charges.
- On Networking, allow the monitored computers' public IP addresses or provide routing and DNS to a private endpoint.
- On Security, require secure transfer and TLS 1.2, disable anonymous access, and keep Enable storage account key access enabled.
- Soft delete and versioning improve recovery but retained data can consume storage. Disable them for predictable quota cleanup or configure suitable lifecycle rules. Avoid immutability policies when old recordings must be deleted.
- Click Review + create, verify the settings, and click Create.

2. Create the private container and obtain a key

- Open Data storage / Containers / + Container. Enter a 3-63 character lowercase name, select Private (no anonymous access), and create the container.
- Open Security + networking / Access keys / Show keys. Copy only the Key under key1 or key2, not the connection string. Protect and rotate this broad-access credential.

3. Configure and test the Azure profile

- Create an Azure Blob Storage profile. Leave HTTPS endpoint empty for `https://<account>.blob.core.windows.net`; use a custom endpoint only for a compatible private endpoint or Azure Stack deployment.
- Enter the exact existing Container, an optional Folder, the Storage account name, and only the copied Key under Account key (Base64).
- Set Recording quota manually or leave it unlimited, then click Save and Test connection.
- Troubleshooting: for AuthenticationFailed, verify the account and key, Shared Key access, and computer clock. For AuthorizationFailure, check firewall and private-network rules. For ContainerNotFound, verify the exact container. If deleted data still occupies storage, check soft delete, versioning, snapshots, lifecycle rules, and immutability. After rotating a key, update the profile and reapply recorder settings.

Azure references: <https://learn.microsoft.com/azure/storage/common/storage-account-create>,
<https://learn.microsoft.com/azure/storage/blobs/blob-containers-portal>,
<https://learn.microsoft.com/azure/storage/common/storage-account-keys-manage>, and
<https://learn.microsoft.com/azure/storage/common/shared-key-authorization-prevent>.

Folder Layout and Migration

```
<folder>/<agent host name>/desktop-recordings/<recording file>  
<folder>/<agent host name>/audio-recordings/<recording file>
```

When an agent changes from local to external storage, existing recordings in its recorder folder are queued for upload in addition to new recordings.

Playback, Pending Uploads, and Offline Access

External recordings are listed by user and date in the normal recordings browser. Playback downloads the selected object to the console recording cache, where it remains available while the agent is offline.

If an upload fails, the completed recording remains in the agent's local .cloud-pending folder and is retried later. Pending recordings can be played while the agent is connected.

Refresh, playback, automatic retention cleanup, and manual deletion operate with the selected external storage profile.

Quota and Storage Usage

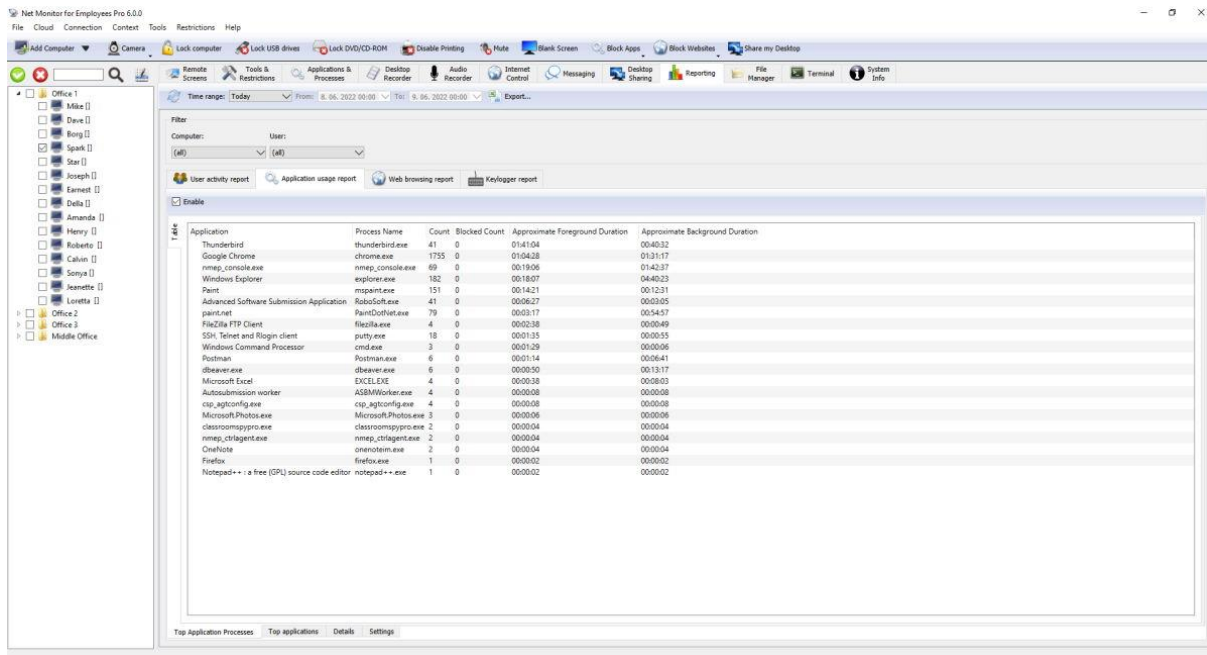
A recording quota can be configured for a profile. When the quota is reached, choose whether to delete the oldest recordings automatically or stop recording and report an error. Desktop Recorder and Audio Recorder display occupied recording space and the configured quota; pending recordings are included in displayed usage.

Detect... can obtain total and available capacity from SMB 2/3, SFTP, and WebDAV servers that report quota information. Enter the recording quota manually when a provider does not expose capacity information.

7.4 Employee Activity Tracker and Monitoring Reports

Reporting can be used to turn collected remote computer activity into clear historical reports and records. This feature allows managers to review employee activity with clear searchable records and use the results for follow-up.

- Reviewing employee active and idle time trends.
- Seeing which apps and websites take most work time.
- Reconstructing a clear timeline for incidents.
- Preparing weekly or monthly reports for team leads and HR.
- Using facts during coaching and performance follow-up.



Screenshot: Reporting and activity tracker view.

Reporting aggregates historical remote computer data into searchable analytics for user activity, application usage, website usage, and keystrokes.

Toolbar and Global Filters

- Refresh loads new records and updates report totals.
- Time range presets include today/yesterday, week/month presets, last 7/14 days, and custom range.
- Filter controls narrow results by computer and user, plus application where relevant.
- Export saves current report output to file.

Reports

- User activity report: shows when the user was active or idle, plus logon/logoff timeline. Use this report to understand real working time for each employee.
- Application usage report: shows which applications and processes were used most. Use this report to see if employees spend time in approved work software.

- Web browsing report: shows visited websites and full URLs. Use this report to review work-related browsing and identify non-work browsing.
- Keylogger report: shows captured typed text and key sequences. Use this report when you need detailed activity evidence for investigations.

Settings in Each Report

- Enable turns logging on or off for that report type.
- Save configuration persists settings.
- Retention settings can remove old records on remote computers and in local console archive.
- External logger can send report events as JSON to another web address, with an optional header key and value.

External Logger JSON Examples

External logger sends JSON data to your configured URL using HTTP POST and Content-Type: application/json; charset=utf-8. If you set a custom header key/value in the UI, that header is also sent. Each payload also includes computer/session fields such as host, hwid, user, userfullname, ntdomain, terminal, session, ipv4, ipv6, pipv4, and pipv6.

User activity report event

```
{
  "time": "2026-04-29T08:45:10+02:00",
  "event": "Active",
  "duration": 300,
  "pid": 9152,
  "executable": "OUTLOOK.EXE",
  "name": "Microsoft Outlook",
  "caption": "Inbox - Outlook",
  "update": true,
  "host": "PC-01",
  "user": "j.smith",
  "session": 1
}
```

Application usage report event

```
{
  "time": "2026-04-29T09:10:00+02:00",
  "event": "InForeground",
  "pid": 14520,
  "executable": "excel.exe",
  "name": "Microsoft Excel",
  "caption": "Q2 Budget.xlsx - Excel",
  "class": "XLMMAIN",
  "cmd": "\"C:\\Program Files\\Microsoft Office\\root\\Office16\\EXCEL.EXE\" \"C:\\Reports\\Q2 Budget.xlsx\"",
  "host": "PC-01",
  "user": "j.smith",
  "session": 1
}
```

Web browsing report event

```
{
  "time": "2026-04-29T09:22:14+02:00",
  "event": "Opened",
  "pid": 14520,
  "url": "https://portal.company.com/tickets/12345",
  "title": "Ticket #12345 - Company Portal",
  "browser": "chrome.exe",
  "host": "PC-01",
  "user": "j.smith",
  "session": 1
}
```

Keylogger report event

```
{
  "time": "2026-04-29T09:25:51+02:00",
  "pid": 9152,
  "name": "Microsoft Outlook",
  "executable": "OUTLOOK.EXE",
  "class": "rctrl_renwnd32",
  "caption": "New Message - Outlook",
  "keystrokes": "Hello team{{Return}}",
  "host": "PC-01",
  "user": "j.smith",
  "session": 1
}
```

Some fields are sent only in specific situations, for example duration on close/background events, or update on user-duration updates.

How Reporting Works

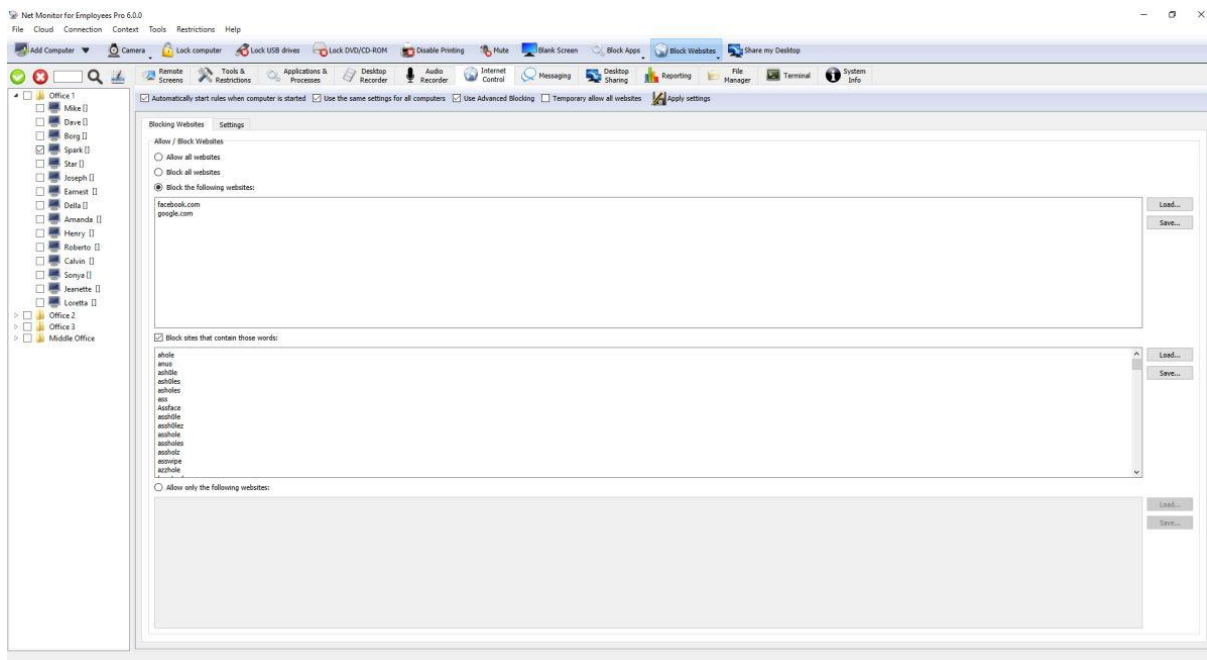
- Console downloads logs from connected remote computers into local report storage.
- Report totals and charts are updated from downloaded records.
- Status indicators show when data is loading, processing, or exporting.

8. Internet Control, Messaging, and Desktop Sharing

8.1 Internet Blocking Software for Employee Computers

Internet Monitor can be used to enforce website access policy with centralized allow and block rules. This feature allows managers to reduce distractions and block risky websites while still allowing approved work websites.

- Blocking social media, streaming, or gaming websites during work hours.
- Allowing only required business websites for specific teams.
- Applying strict website rules during exams, training, or onboarding.
- Temporarily opening access for troubleshooting and then restoring policy.
- Reducing security risk by blocking known dangerous websites.



Screenshot: Internet Control settings.

Internet Control enforces website policy on remote computers with allow/block modes, URL and keyword lists, and configurable blocked-site actions.

Top Bar Settings

- Automatically start rules when computer is started makes policy persistent after restart.
- Use the same settings for all computers applies one global profile instead of per-computer policy.
- Use Advanced Blocking enables lower-level filtering behavior.
- Temporary allow all websites temporarily bypasses blocking until policy is re-applied.
- Apply settings confirms and pushes current configuration.

Blocking Websites Tab

- Choose how internet access should work: allow all websites, block all websites, block only listed websites, or allow only listed websites.

- Add website addresses to your allow list or block list.
- Use Load and Save to import or export website lists.
- Block sites that contain those words blocks websites that include selected words in the address.

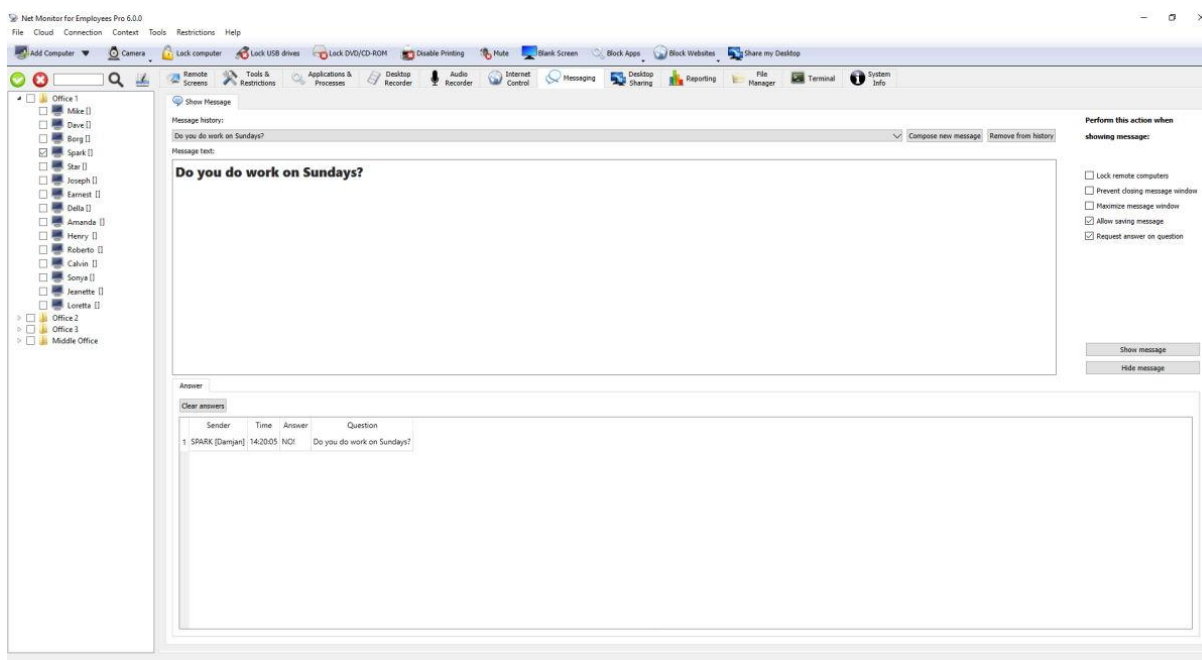
Settings Tab — Blocked-Site Behavior

- Show message: display custom message in browser.
- Redirect: redirect browser to configured URL.
- Close browser: closes browser that opened blocked website.

8.2 Employee Messaging Software for Remote Computer Alerts

Messaging can be used to send messages or questions to selected users and collect responses. This feature allows managers to make sure employees see important messages and confirm them when needed.

- Sending urgent instructions to all selected computers.
- Requesting confirmation that employees read a policy update.
- Collecting quick status answers from remote employees.
- Sending shift-start reminders to distributed teams.
- Notifying users about planned downtime or maintenance windows.



Screenshot: Messaging tab.

Messaging sends announcements or questions to selected computers and can collect user answers in real time.

Compose and Reuse Messages

- Message history stores reusable templates.
- Compose new message starts a fresh draft.
- Remove from history deletes selected template.
- Message text supports formatted content.

Show Message Options

- Lock remote computers blocks workstation input while message is visible.
- Prevent closing message window keeps message on screen until admin hides it.
- Maximize message window shows message fullscreen.
- Allow saving message enables remote computer copy/save actions.
- Request answer on question shows answer field and sends answers back to console.

Show / Hide Workflow

41. Prepare message text and options.
42. Click Show message to display on selected remote computers.
43. Click Hide message to close active message windows remotely.

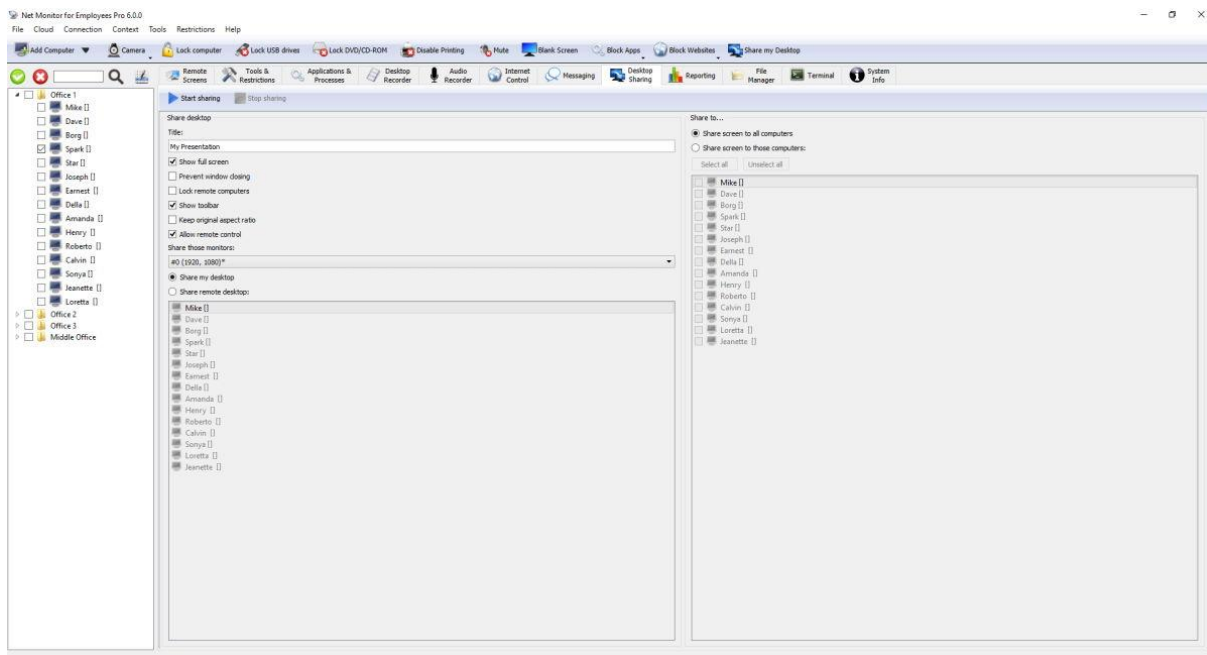
Answers Tab

- Answers table shows sender, time, answer text, and related question.
- If answer is required, remote computer user is prompted until answer is submitted.
- Clear answers removes collected answers from current console view.

8.3 Share Desktop for Remote Presentation and Training

Desktop Sharing can be used to show one screen on all selected computers at the same time. This feature allows you to centralize demonstrations and communication with controls for viewer behavior and permissions.

- Running employee onboarding and training sessions.
- Showing a new workflow to all selected computers at once.
- Presenting urgent security instructions during incidents.
- Sharing one employee screen as a best-practice example.
- Guiding exam or classroom users through the same steps together.



Screenshot: Desktop Sharing configuration.

Desktop Sharing sends the presenter screen to all selected computers. You can share your own desktop or share one selected remote computer screen to all selected computers.

Source Selection — What You Share

- Share my desktop uses the local console screen as source.
- Share remote desktop uses one connected remote computer as the source screen.
- Share those monitors selects all monitors or a specific monitor from source side.
- Present on this monitor selects where presenter window opens on your workstation.

Target Selection — Who Receives

- Share screen to all computers sends the session to all connected targets.
- Share screen to those computers enables manual target list.
- Select all and Unselect all speed up list management.

Session Options Explained

- Title sets the text users see in the sharing window title bar.
- Show full screen opens the shared desktop in full-screen mode on employee computers.
- Prevent window closing stops users from closing the sharing window during the session.
- Lock remote computers blocks normal keyboard and mouse usage so users stay focused on the presentation.
- Show toolbar shows the sharing toolbar in the viewer window.
- Keep original aspect ratio keeps the screen shape correct and avoids stretched image.
- Allow remote control lets participants control the shared screen with keyboard and mouse when needed.
- Allow saving a screenshot lets participants save a screenshot from the shared session.
- Start sharing starts the session on all selected computers after confirmation.
- Stop sharing ends the session on all selected computers immediately.

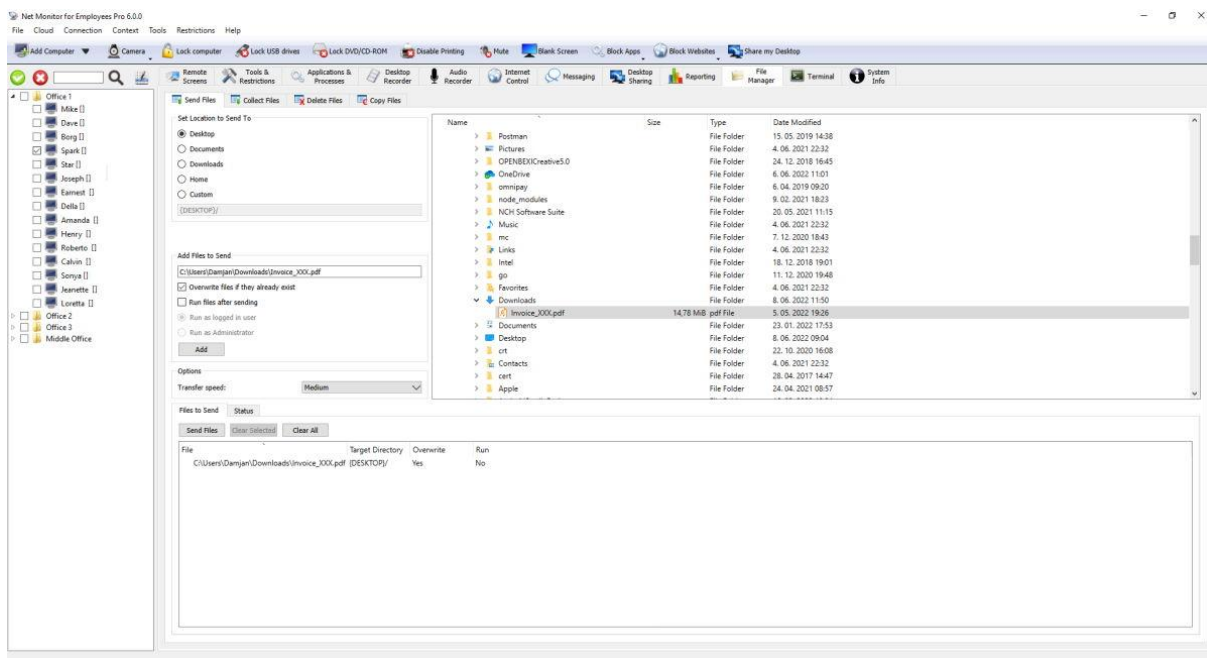
9. File and Administrative Tools

9.1 Remote File Manager for Employee Computers

File Manager can be used for managed remote file operations without opening full remote control sessions. This feature allows managers to send, collect, copy, and delete files on remote computers in a controlled way.

- Sending work documents, scripts, or updates to employee computers.
- Collecting logs, screenshots, and exported files for investigation.
- Copying incident evidence from remote computers to the manager console.
- Removing unauthorized files from selected computers.
- Distributing policy documents to all selected computers before an audit.

Send Files Tab

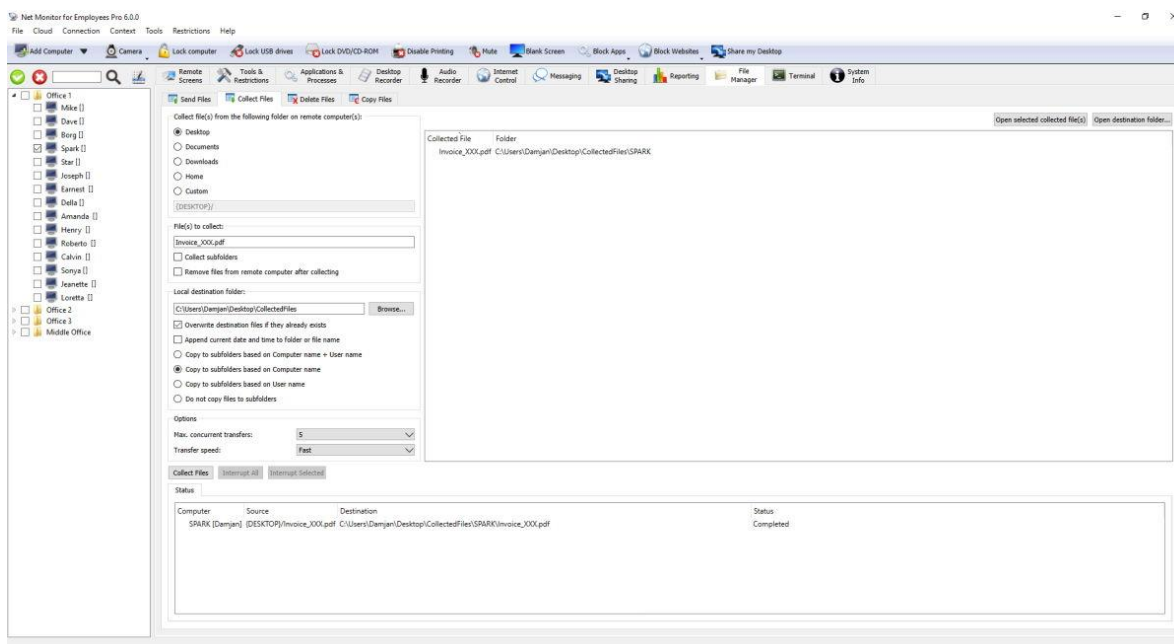


Screenshot: Send Files tab.

Upload one or more local files to selected remote computers.

- Choose destination folder (Desktop/Documents/Downloads/Home/Custom) to decide where files are saved.
- Choose what should happen if a file with the same name already exists.
- Set transfer speed (Slow/Medium/Fast) to control how quickly files are sent.
- Run files after sending starts the file only after it is fully transferred.
- Run as Administrator runs the file with higher permissions; otherwise it runs as the current logged user.
- Status tab shows current progress and lets you stop selected transfers or all transfers.

Collect Files Tab

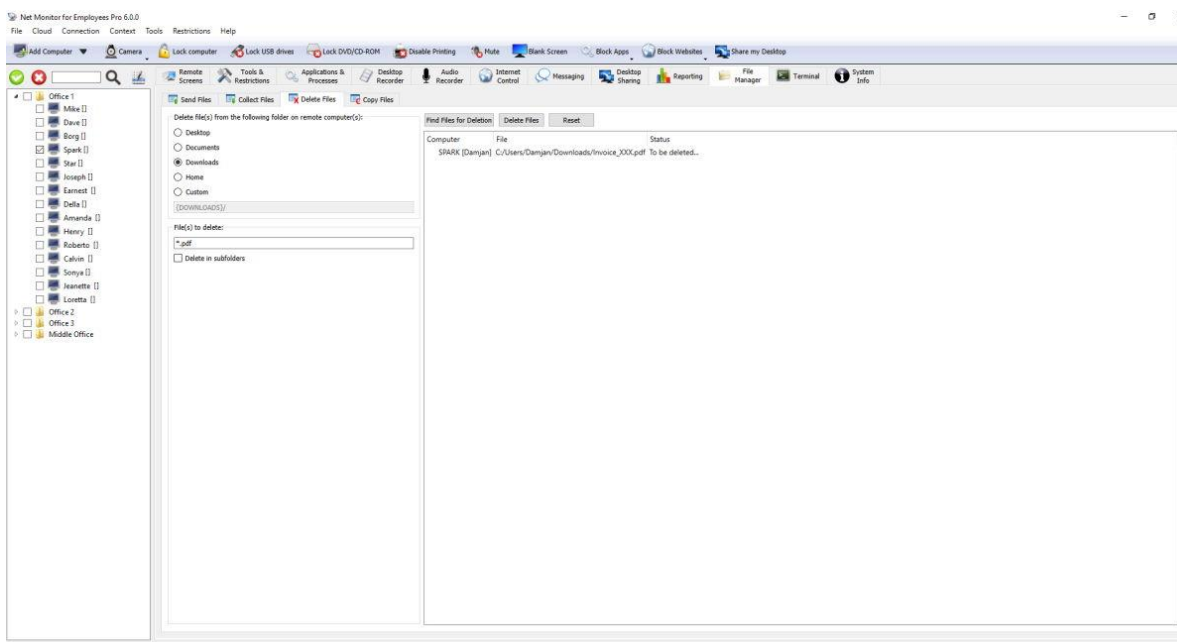


Screenshot: Collect Files tab.

Download files from remote computers to console storage.

- You can collect one exact file name or use file patterns such as *.log.
- Use VSS helps copy files that are currently locked by another program on supported systems.
- You can limit how many transfers run at the same time. Extra files wait and continue automatically.
- Choose how downloaded folders are organized: by computer, by user, by both, or flat in one folder.
- You can append date to file names, overwrite existing files, or remove remote files after collect.
- If connection is interrupted, unfinished downloads continue after reconnect.

Delete Files Tab



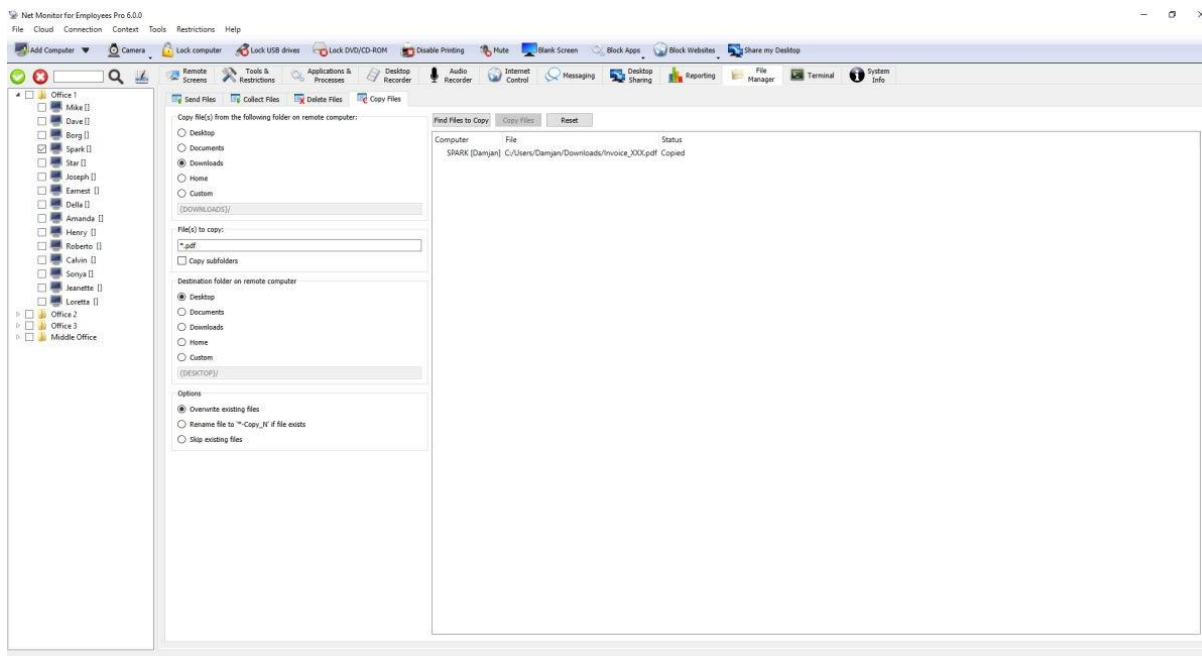
Screenshot: Delete Files tab.

This tab uses a two-step safety flow: list first, then delete from the confirmed list.

44. Set source folder and file patterns.
45. Run Find Files for Deletion to preview candidates.
46. Execute Delete Files on the generated list.

Delete in subfolders also finds matching files inside subfolders before deletion.

Copy Files Tab



Screenshot: Copy Files tab.

Copy files between folders on the same remote computer.

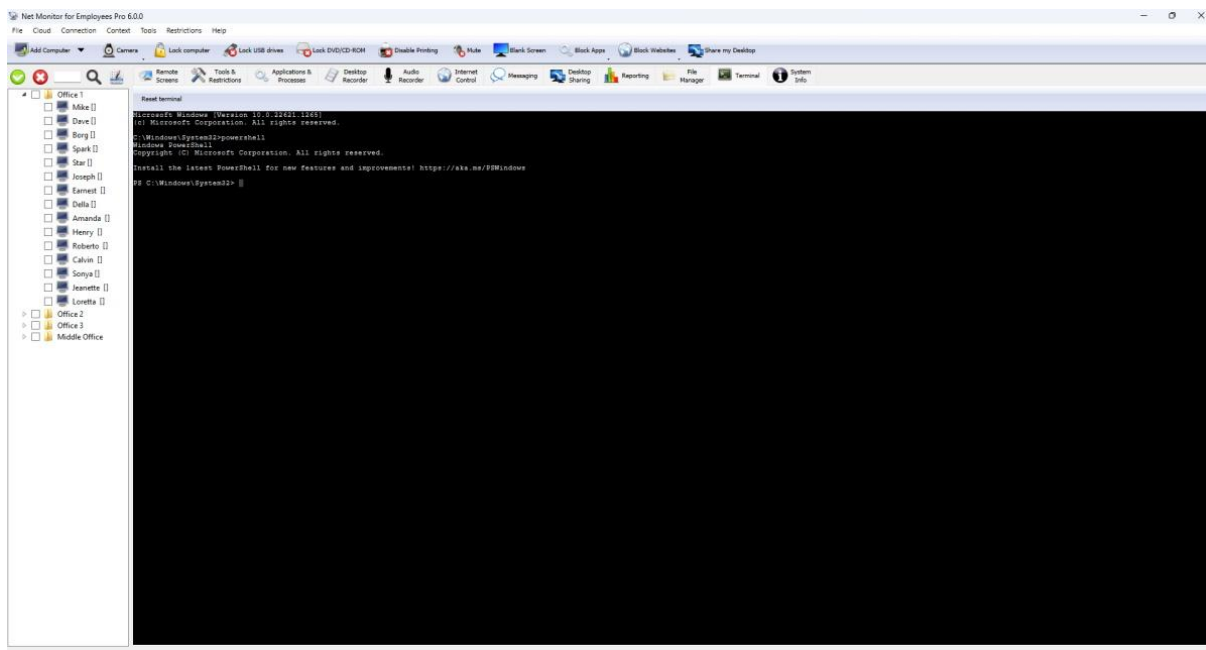
47. Choose source and pattern(s).
48. Run Find Files to Copy to preview.
49. Set destination and conflict mode (overwrite/rename/skip).
50. Run copy action.

Conflict mode decides what happens if the target file already exists: overwrite replaces it, rename creates a copy with a new name, and skip leaves the existing file unchanged. VSS copy mode is available for locked files where supported.

9.2 Remote Terminal CMD PowerShell Bash

Terminal can be used to check problems and run commands directly on remote computers. This feature allows managers and support staff to troubleshoot quickly without opening full remote control.

- Running quick checks on employee computers without opening full remote control.
- Collecting logs and service status during incident investigation.
- Running shell commands on selected computers.
- Applying fast fixes when employees report technical issues.
- Verifying that policy or software changes were applied correctly.



Screenshot: Remote Terminal tab.

Terminal opens an interactive shell on the selected remote computer, for example cmd.exe on Windows or /bin/bash on Linux/macOS.

What You Can Do In This Screen

- Run commands interactively on the selected connected computer.
- Use Reset terminal to stop the current shell and start a clean shell session.
- Switch between computers while keeping each session output separated.

How Terminal Sessions Work

- When Terminal tab is selected, the console starts a terminal session automatically for the current connected remote computer.
- Keyboard input is sent directly to the remote computer shell, and results appear in real time.
- Terminal window resize keeps the shell display readable in full-screen and split views.
- Each remote computer keeps its own command output, so switching computers does not mix history.

When To Use Reset Terminal

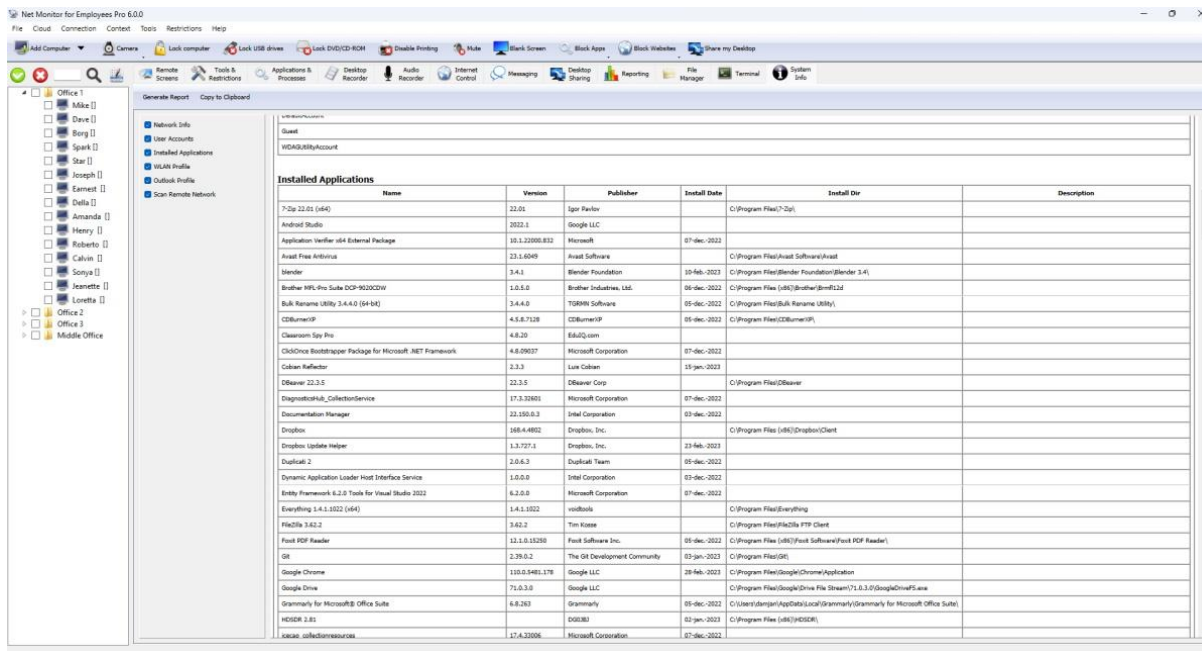
Use Reset terminal when the shell looks stuck, prompt is broken, or output stops unexpectedly. Reset starts a fresh shell. If the remote computer shell exits on its own, the terminal session is restarted automatically.

9.3 Remote System Information and Computer Inventory

System Info can be used to collect hardware, software, and network inventory from remote computers into one report. This feature allows managers to collect clear computer details for support, audits, and employee follow-up without checking each machine manually.

- Checking employee computer details before remote troubleshooting.
- Finding missing software, outdated versions, or unsupported hardware.
- Troubleshooting network and account configuration problems.

- Preparing compliance and asset-inventory reports.
- Comparing multiple employee computers to spot configuration differences.



Screenshot: System Information and inventory report screen.

Generate structured system/inventory reports from selected remote computers. Reports are built step by step and update as each remote computer sends data.

What This Screen Gives You

- Generate Report requests selected sections from all selected connected remote computers.
- Copy to Clipboard copies current report output for ticketing, audits, and documentation.
- Checkboxes control exactly which report sections are queried.

Report Sections Explained

- Network Info: external IP plus network interfaces and IP/subnet details.
- User Accounts: local user accounts found on remote computer.
- Installed Applications: app name, version, publisher, install date, directory, description.
- WLAN Profile: profile name, authentication, encryption, and key fields.
- Outlook Profile: account and server profile data.
- Scan Remote Network: discovered hosts with IP, host name, MAC, and vendor mapping.

Recommended Workflow

51. Select target remote computers in the tree.
52. Check only reports needed for this task.
53. Click Generate Report and wait for responses.
54. Export quickly with Copy to Clipboard.

Important notes: Remote network scan can run longer than other sections and results appear progressively. Some sections may include sensitive values, such as WLAN keys or profile credentials.

10. Remote Desktop Control

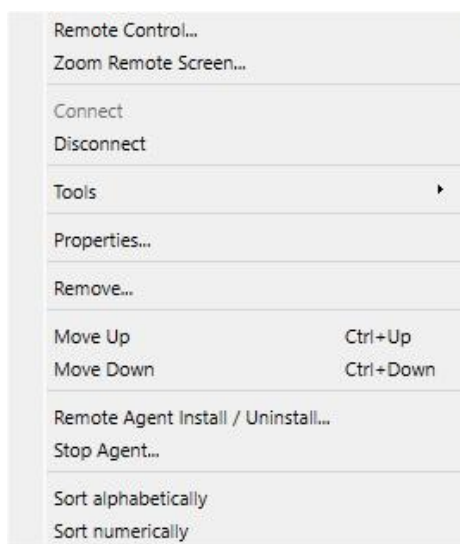
Remote Control can be used for direct hands-on support when a manager or technician needs to use keyboard and mouse on a remote computer. This feature allows you to reduce time to resolution by fixing issues in the exact user context.

- Helping an employee fix a problem in real time.
- Completing blocked updates or configuration steps remotely.
- Showing an employee the correct workflow step by step.
- Verifying suspicious behavior while the employee is online.
- Confirming immediately that a fix worked before ending the session.

Remote Desktop Control

Open a live keyboard and mouse session for the selected remote computer. You can start from the Object Menu in the computer tree or from remote-screen actions.

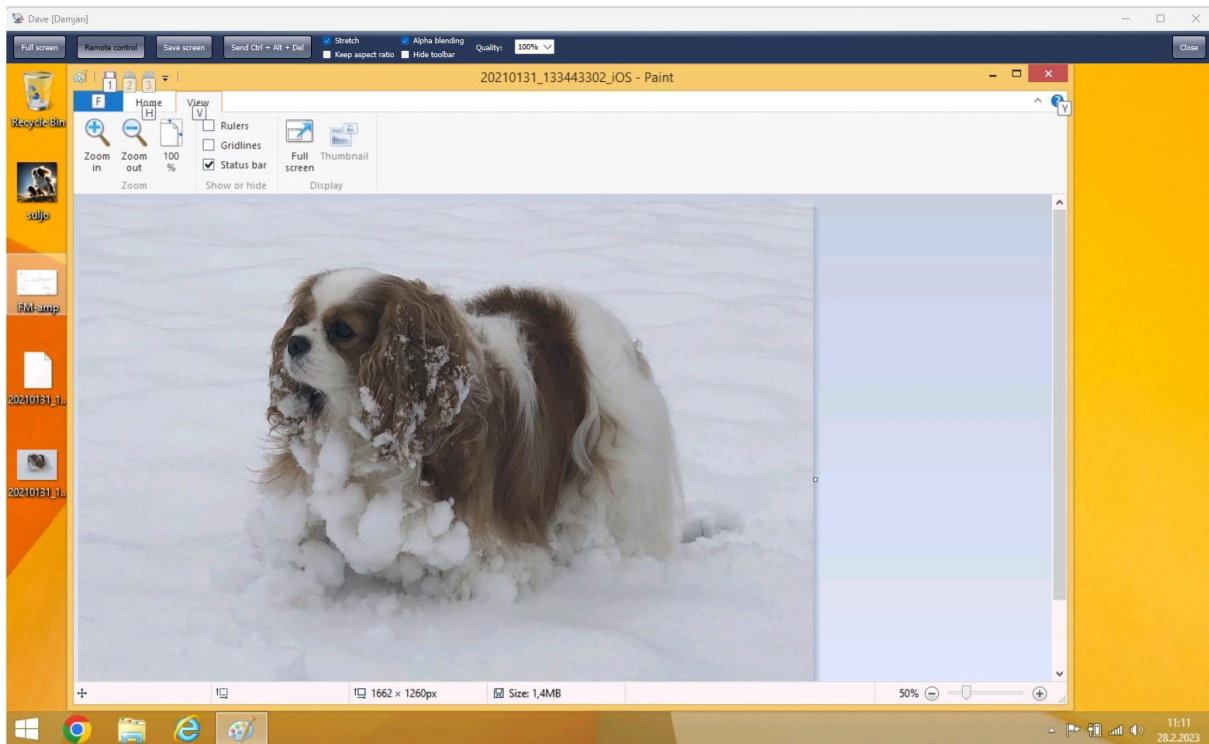
Start Session From Object Menu



Screenshot: Object Menu with Remote Control option.

- Right-click a connected computer/session and choose Remote Control.
- Console asks for confirmation before taking over keyboard and mouse.
- Use Zoom Remote Screen when you need view-only mode.

Remote Control Window Controls



Screenshot: Remote Control window.

- Full screen toggles fullscreen mode.
- Remote control enables/disables keyboard and mouse takeover during session.
- Send Ctrl + Alt + Del sends this key combination to the remote computer.
- Display selects monitor when the remote computer has multiple displays.
- Stretch, Keep aspect ratio, Alpha blending, and Quality adjust image look and speed.
- Hide toolbar auto-hides controls and shows them again when the cursor reaches the top edge.
- Save screenshot saves the current remote screen image.

Session Notes

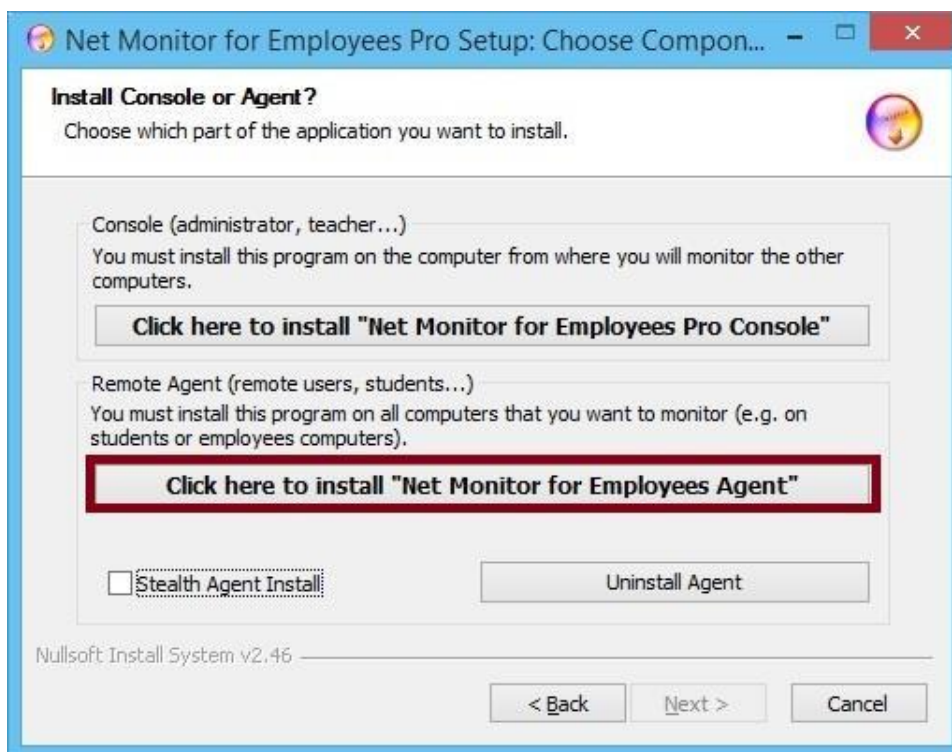
- Common display quality/aspect options are reused in next sessions.
- Closing the remote-control window releases control and console monitoring continues.

11. Mobile Console for iOS and Android

The mobile console lets you monitor and control employee computers from a smartphone or tablet. Agent is currently supported only on desktop operating systems.

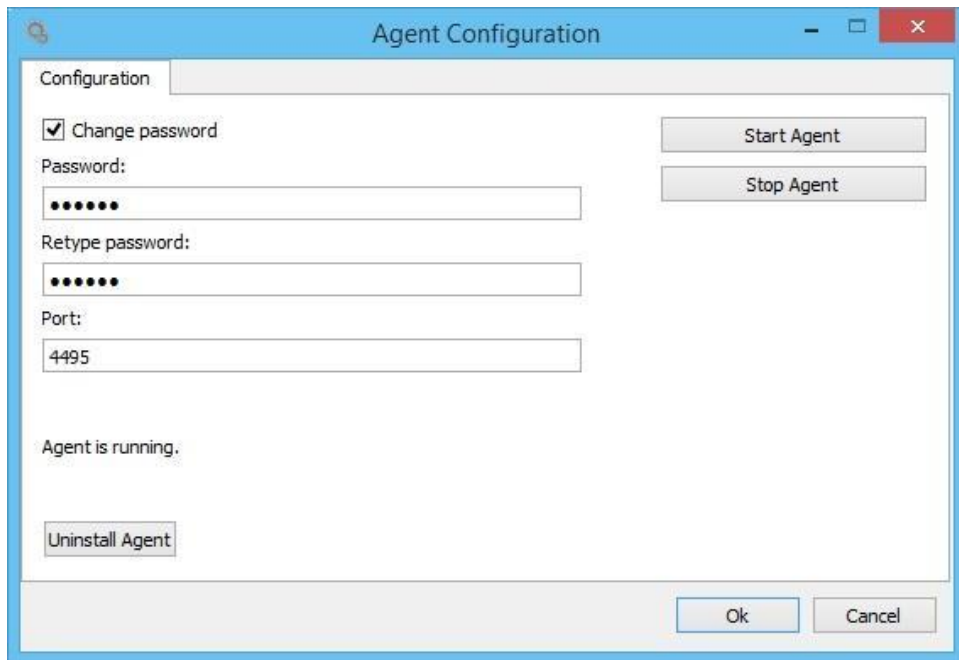
11.1 Install Agent

Before you can start controlling and monitoring a network PC, install an agent on it. Download the desktop package that contains Console and Agent, then start installation on the PC that you want to monitor. After the initial installer screens, choose what to install. Choose the second option to install an agent.



Screenshot: Windows agent install choice.

Proceed with agent installation until the configuration screen is displayed. Choose the password that you want to use when adding the agent to the console. The recommended practice is to use the same password for all network PCs. Remember the password because it is needed in the next step. Finish installation. Repeat this step for all network PCs that you want to control.



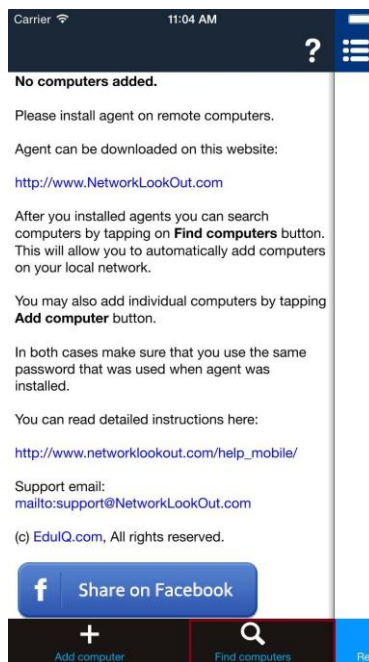
Screenshot: Windows agent configuration for mobile console use.

11.2 Find and Add PCs Where Agent Is Installed

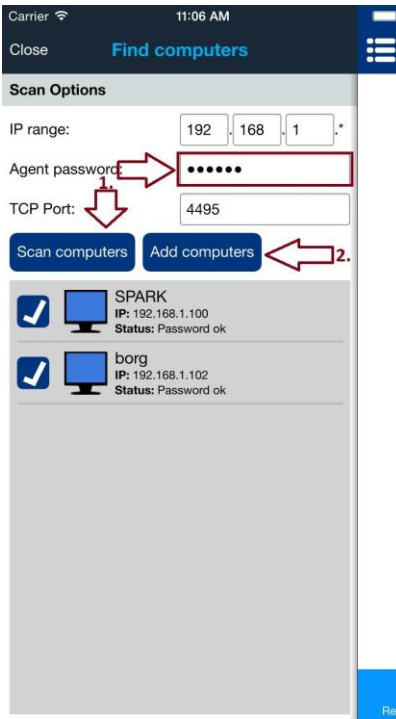
Open the console on your smartphone or tablet and tap Find computers. On the next screen, enter the agent password chosen during agent installation. Tap Scan computers and wait a few seconds for network PCs to be discovered. If nothing is discovered, check your Wi-Fi connection and tap Scan computers again.

Note: You can scan PCs only on your local network. If they are not discovered, add them manually.

If PCs are discovered, select which PCs to add and then tap Add computers.



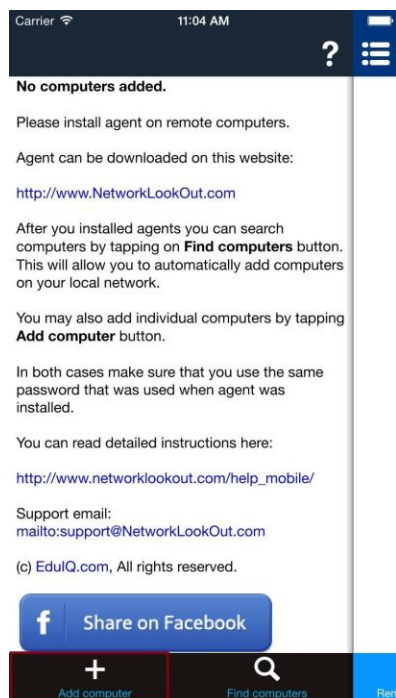
Screenshot: Find computers button on mobile console.



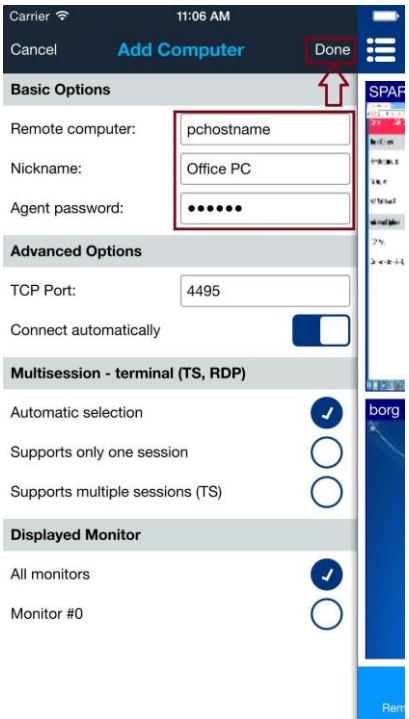
Screenshot: Scan network and add discovered computers.

11.3 Manually Add Computers

If PCs are on a different network or were not automatically discovered, add them manually by tapping Add computer. On the next screen, fill all required fields. Under Remote computer, type the IP or DNS host name of the network PC. Enter the agent password chosen in the first step when installing the agent. When everything is filled correctly, tap Done.



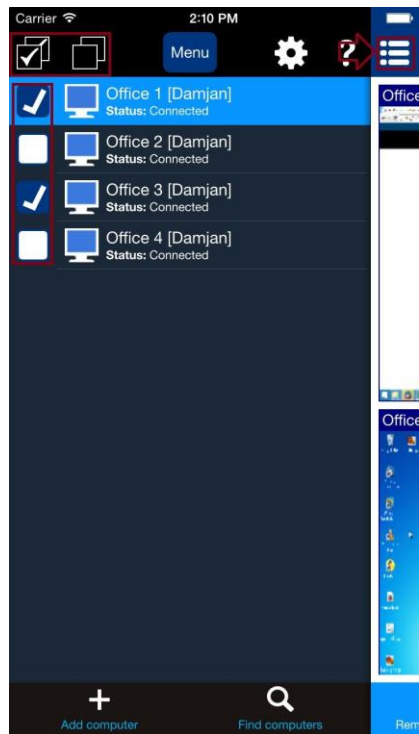
Screenshot: Add computer button on mobile console.



Screenshot: Manually add computer screen.

11.4 Computer List View

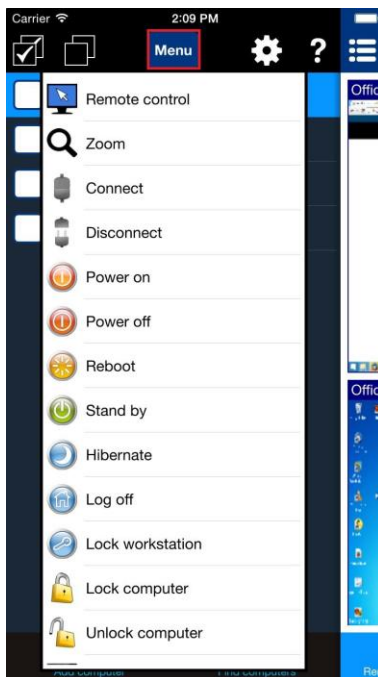
All added PCs appear in a list. You can select one computer by tapping it. To select more computers, use checkboxes. The computer list can be hidden by tapping the menu icon.



Screenshot: Mobile computer list navigation and selection.

11.5 Action Menu

Action menu can be used to invoke specific actions on selected network computers. Show the menu by tapping Menu or by tap-and-hold on a specific computer in the list.



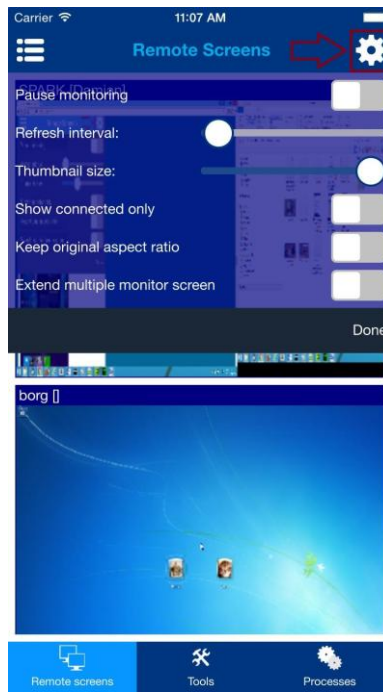
Screenshot: Mobile action menu.

11.6 Remote Screens View

Remote computer screens can be viewed using Remote screens view. On smartphones, hide Computer list view first. The configuration menu can be displayed or hidden by tapping the gear icon in the upper-right corner.



Screenshot: Mobile remote screens view.



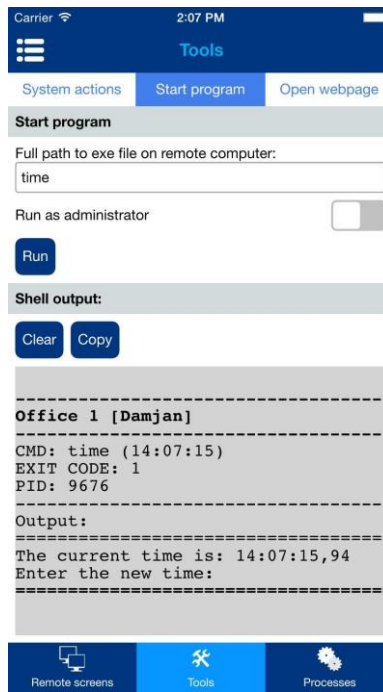
Screenshot: Mobile remote screens settings.

11.7 Tools View

Several useful actions can be performed on remote computers. Before executing actions, make sure you select the desired computers in Computer list view. You can also start a program on remote computers by tapping the Start program tab.



Screenshot: Mobile tools view.



Screenshot: Mobile Start program tab.

11.8 Processes View

You can see which processes and applications are running on a remote computer. The processes list is displayed for the highlighted computer in Computer list view. The processes list also contains checkboxes that can be selected to perform actions on a group of selected processes or applications.

Process action menu can be displayed by tap-and-hold on a specific process or by sliding left on a specific process. This menu allows you to close the application or kill the process. Additional process actions can be performed using Stop menu by tapping the upper-right corner stop icon. Actions Kill process by name and Stop applications by name can also be performed on all selected computers simultaneously.



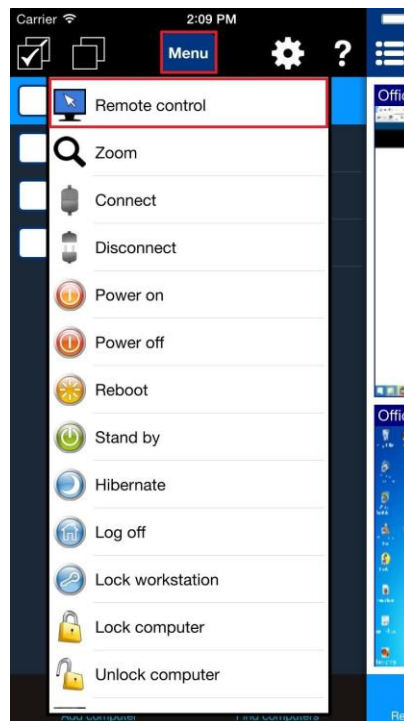
Screenshot: Mobile processes swipe menu.



Screenshot: Mobile processes stop menu.

11.9 Remote Control

You can remotely control computers using mouse and keyboard. Choose action Remote control from the action menu. On the displayed remote view, control the mouse by dragging the displayed on-screen mouse. You can tap specific mouse buttons. You can also display a keyboard or object menu where additional options are available, such as choosing which monitor to control on multi-monitor systems.



Screenshot: Choose Remote Control from mobile action menu.



Screenshot: Mobile remote control view.