

UserLock 4.0 feature breakdown

This is the detail of all new features in UserLock 4.0.
In the final release this document will be integrated into the standard help file.

Protected accounts

► Ability to define working hours for protected users

Outside of this(these) timeframe(s), users will be logged off with prior warning. This option improves network security outside of working hours, and also puts a term to backup failures due to files remaining open.

In order to configure *allowed time frames*, the new *Hours* tab is available in protected account/group properties. In case of overtime you can choose to close the session, lock the session or do nothing. For the logoff you can define the Notification length in minutes in the *Logoff settings* section.

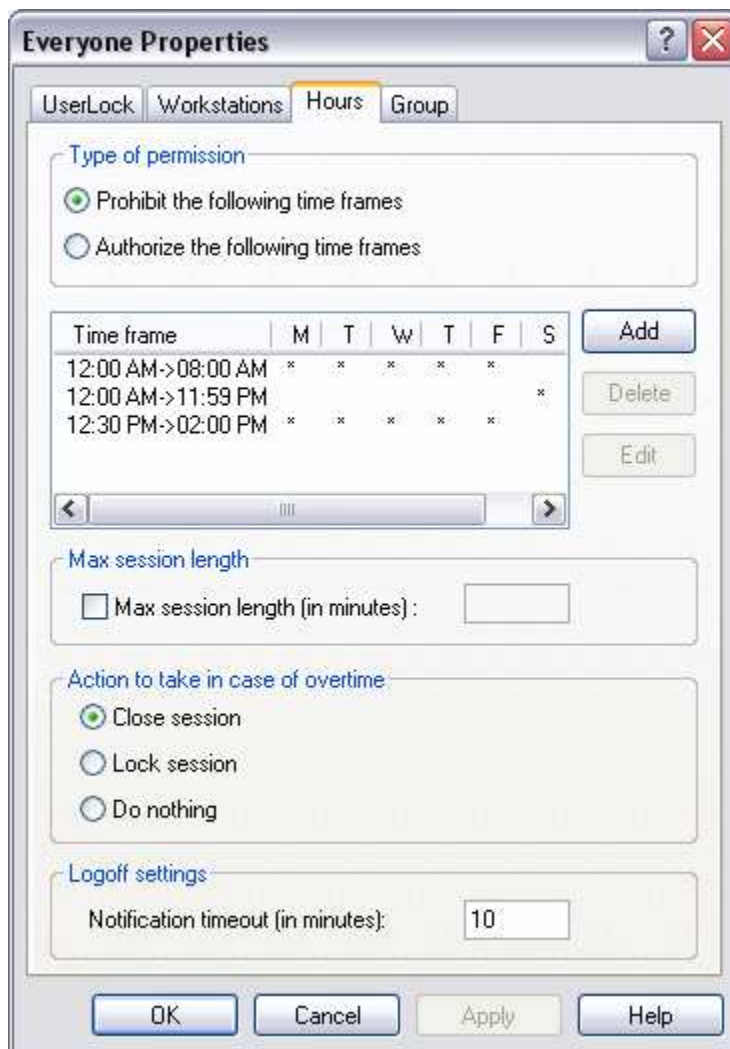


Figure 1 Time frame configuration options

▶ **Ability to define maximum session time for protected users and groups**

When the time is up, users will be logged off with prior warning. This feature will help free access computer sharing and management.

This feature, as well as the logoff notification timeout can be set in the new *Hours* tab in protected account/group properties or in the *Logoff settings* section.

▶ **Ability to define maximum group limits**

In previous versions of UserLock you could only set a limit for the number of sessions for each member of a group. Now you can set limits at group level. This is useful for example if each department of an organization is only allowed to open a limited number of terminal sessions on servers in order to respect shared resource quotas.

To configure these group limits, a new tab is available:

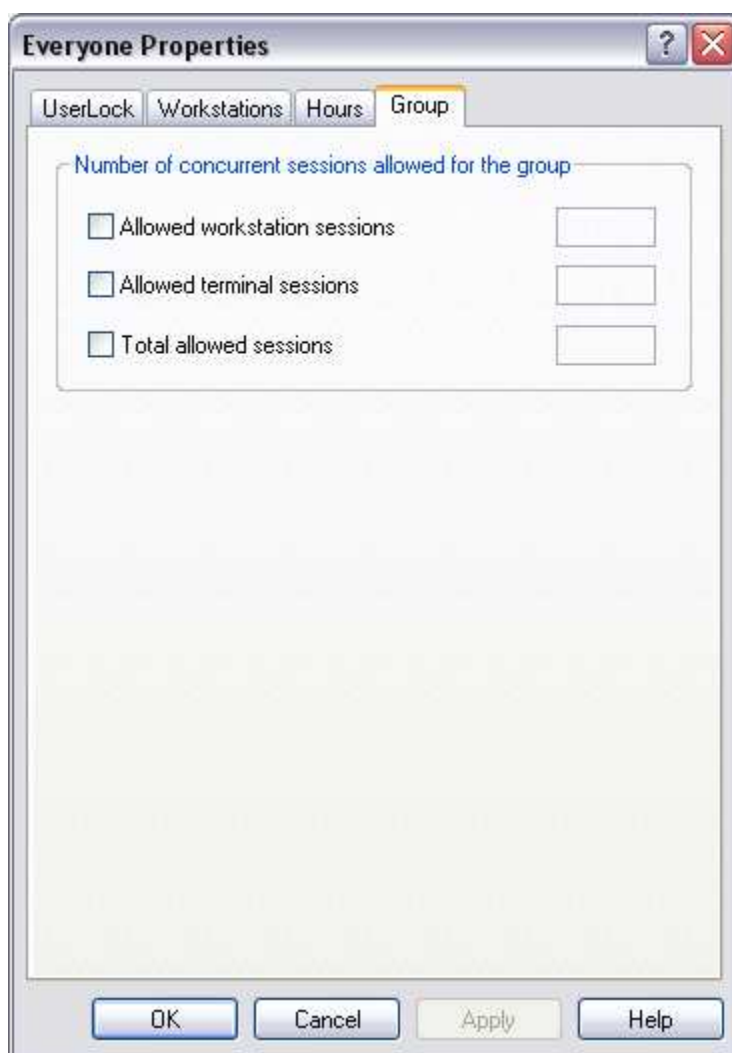


Figure 2 Configure group limits

▶ **The administrator will have the possibility to enable an option allowing users to remotely close their previous session as they logon to another computer.** This will avoid users from having to go back to the previous computer.

In order to configure this, the new check box “Allow to logoff an existing session if the number of allowed sessions has already been reached” is available in the *UserLock* tab of the protected account properties.

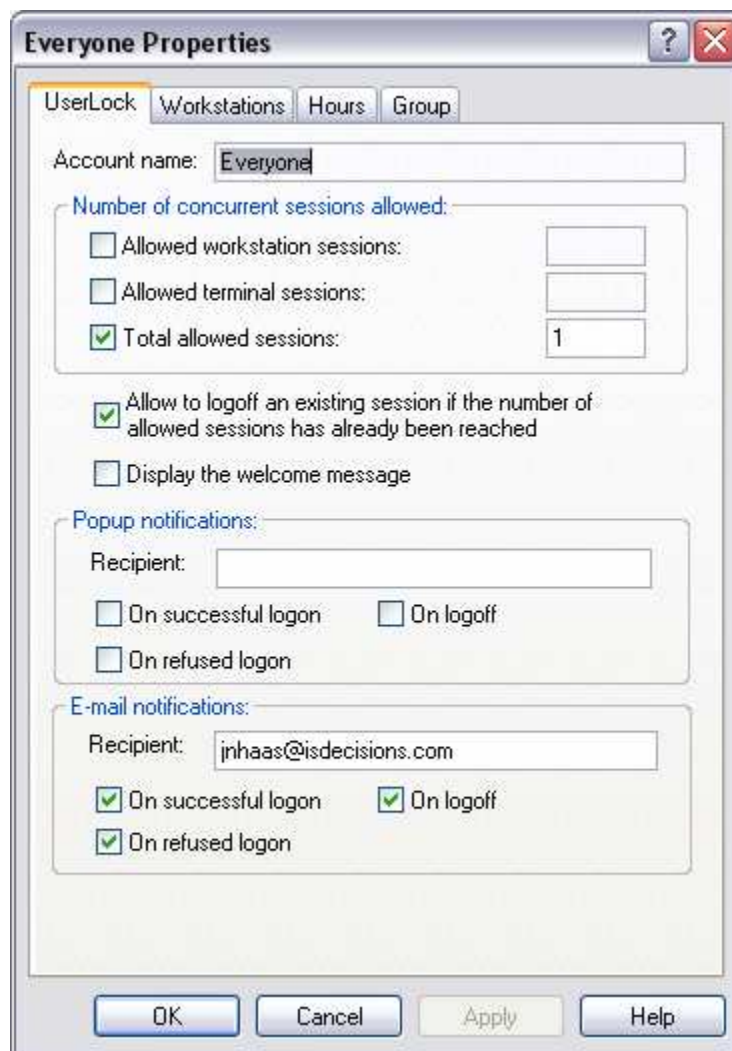


Figure 3 Allow to logoff an exiting session

Server settings

► **New access rights to the UserLock console,** giving certain users the ability to view and manage sessions without having access to more critical UserLock settings such as protected accounts configuration, agent distribution ...

You can configure access rights in the new *Security* tab in server properties. You can only do this with the MMC console and locally (console running on the server).

For example if you want to configure the access for your help desk team so they can reset and logoff user sessions, add the corresponding group and select *Allow* for *User sessions*. All other features in the console (Web and MMC) will be disabled for these users.



Figure 4 Configure access permissions to the console

► Ability to breakdown the computer name syntax into a readable format for all and therefore easily locate the computer.

Ideal for academic or large size networks who most often apply a naming convention for their systems

E.G.: BBBRRRXXX B = Building, R = Room, X = computer number

Computer B12R06X15 is in room 6 of building 12

You can figure the localization mask in server properties.

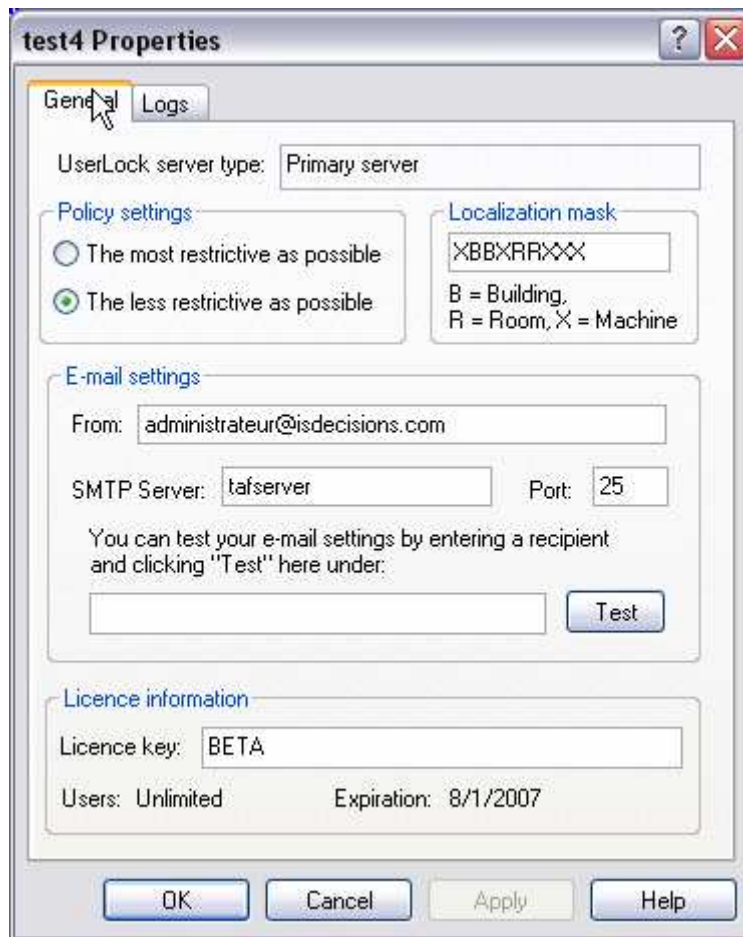


Figure 5 configure the localization mask

Web console/MMC console common new features

► Customize the console's User sessions display screen

- Display sessions per system
- Display users/systems for active sessions only
- Display users/systems for unlocked sessions only
- Display sessions on unavailable systems only
- Display sessions per room/building (depending on computer name syntax), or by Organizational Unit

In the MMC console, you can change the view and the filter with the User sessions context menu (View sub menu).

To configure the filter and the view in the web console just click on the filter bar (click on the +) in order to expand all filter settings (see the screenshot in the Web console section).

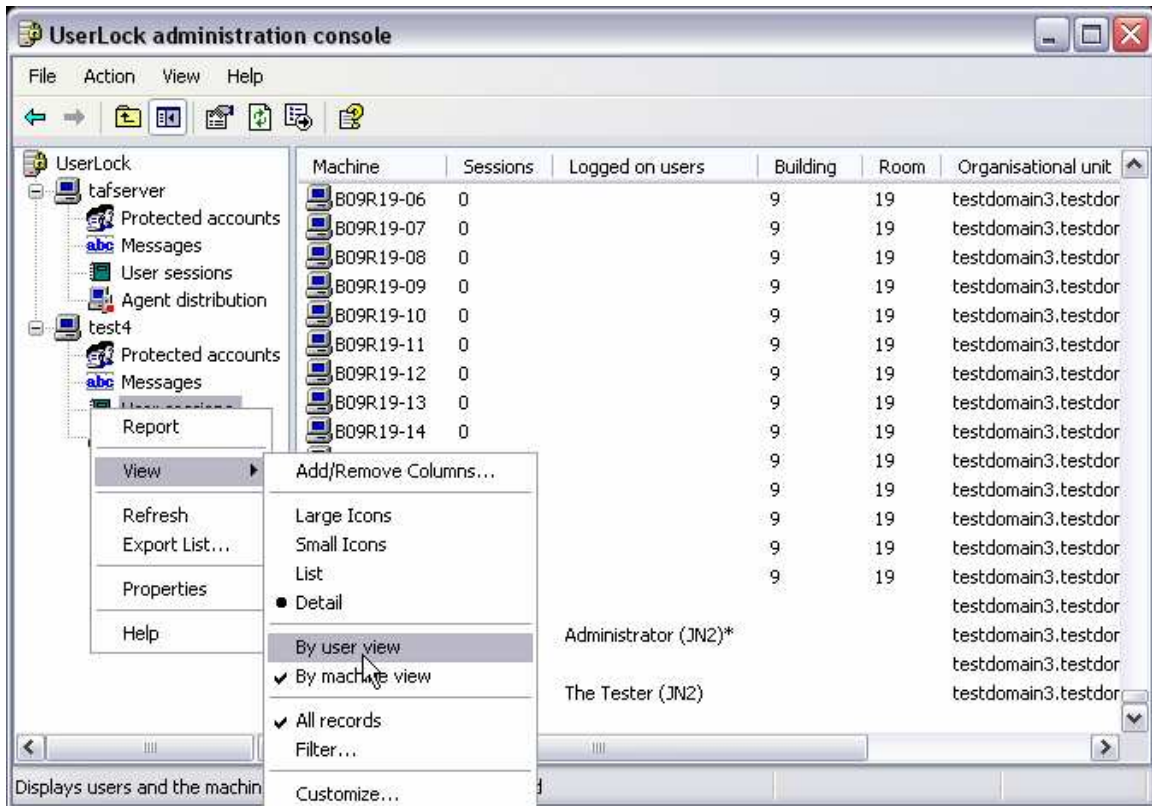


Figure 6 Change the user sessions view in the MMC console

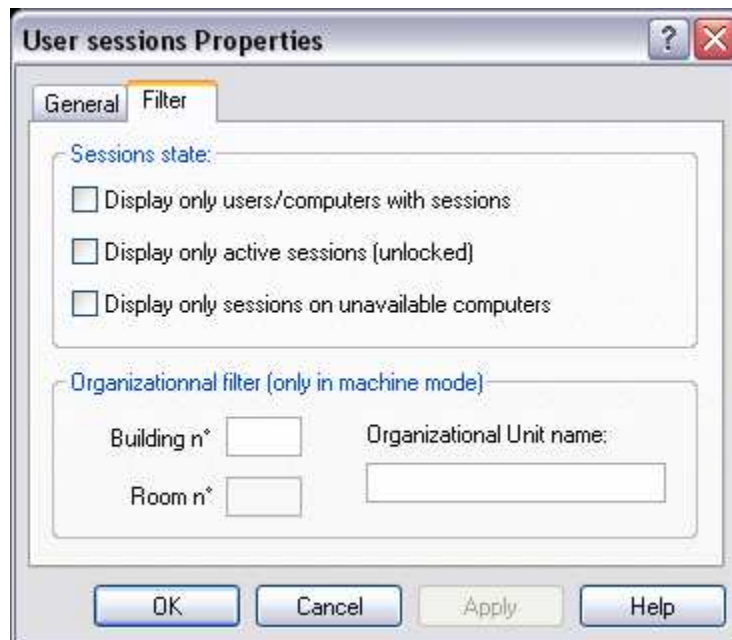


Figure 7 Change the user sessions filter in the MMC console

► Select several sessions at a time from the MMC console to reinitialize/lock/unlock/close simultaneously (already available in the Web interface).

Reinitialize an individual session for a multi-session user from the MMC console (already available in the web interface).

► **Ability to customize the systems displayed in the agent distribution screen**

- Display unavailable systems only
- Display systems without the agent only
- Display systems per room/building (depending on computer name syntax), or by Organizational Unit

In the MMC, you can configure the filter with the Agent distribution context menu (View sub menu).

To configure the filter in the web console just click on the filter bar (click on the +) in order to expand all filter settings (see the screenshot in the Web console section).



Figure 8 Change the agent distribution filter in the MMC console

► **Enhanced user display**

UserLock will now display the user “display name” in the administration console (MMC and web) and in the reports instead of the user account.

Web console

► **Enhanced web console**

The web console can now display the user sessions result and the agent distribution result in pages allowing to manage big networks faster (see screenshot below).

Welcome TESTDOMAIN3\jnh
Server: TEST4

Server Properties Register server...

Protected accounts Messages **User sessions** Agent distribution

Refresh Reports Reset Logoff Lock

Filter Display all users/computers User count: 4 Session count: 2

Select/unselect all sessions << previous 1/1 next >> Display 25 users/pages Ok

User	Sessions	Workstations logged on	Last workstation logged on	Time of last logon	Last workstation logged off	Time of last logoff
The Admin	0		TEST4/JN2	3/22/2007 4:42:11 PM	TEST4/JN2	3/22/2007 5:19:12 PM
Administrator	1	<input type="checkbox"/> TEST4/JN2	TEST4/JN2	3/29/2007 2:32:43 PM	TEST4/JN2	3/28/2007 9:00:53 PM
The Tester	1	<input checked="" type="checkbox"/> TEST6/JN2	TEST6/JN2	3/29/2007 6:17:20 PM	TEST6/JN2	3/28/2007 10:15:08 AM
Le Testeur	0		TEST6/JN2	3/20/2007 6:13:20 PM	TEST6/JN2	3/21/2007 4:10:57 PM

Select/unselect all sessions << previous 1/1 next >> Display 25 users/pages Ok

Filter Display all users/computers User count: 4 Session count: 2

PropertyServer/Properties.asp?onglet=1 Local intranet 100%

Figure 9 User sessions in the web console (filter bar not expanded)

Welcome TESTDOMAIN3\jnh
Server: TEST4

Server Properties Register server...

Protected accounts Messages **User sessions** Agent distribution

Refresh Reports Reset Logoff Lock

Filter **Display all users/computers** User count: 4 Session count: 2

View type: By user view Sessions state: Display all users/computers

Select/unselect all sessions << previous 1/1 next >> Display 25 users/pages Ok

User	Sessions	Workstations logged on	Last workstation logged on	Time of last logon	Last workstation logged off	Time of last logoff
The Admin	0		TEST4/JN2	3/22/2007 4:42:11 PM	TEST4/JN2	3/22/2007 5:19:12 PM
Administrator	1	<input type="checkbox"/> TEST4/JN2	TEST4/JN2	3/29/2007 2:32:43 PM	TEST4/JN2	3/28/2007 9:00:53 PM
The Tester	1	<input type="checkbox"/> TEST6/JN2	TEST6/JN2	3/29/2007 6:17:20 PM	TEST6/JN2	3/28/2007 10:15:08 AM
Le Testeur	0		TEST6/JN2	3/20/2007 6:13:20 PM	TEST6/JN2	3/21/2007 4:10:57 PM

Select/unselect all sessions << previous 1/1 next >> Display 25 users/pages Ok

Local intranet 100%

Figure 10 User sessions in the web console (the filter bar is expanded)

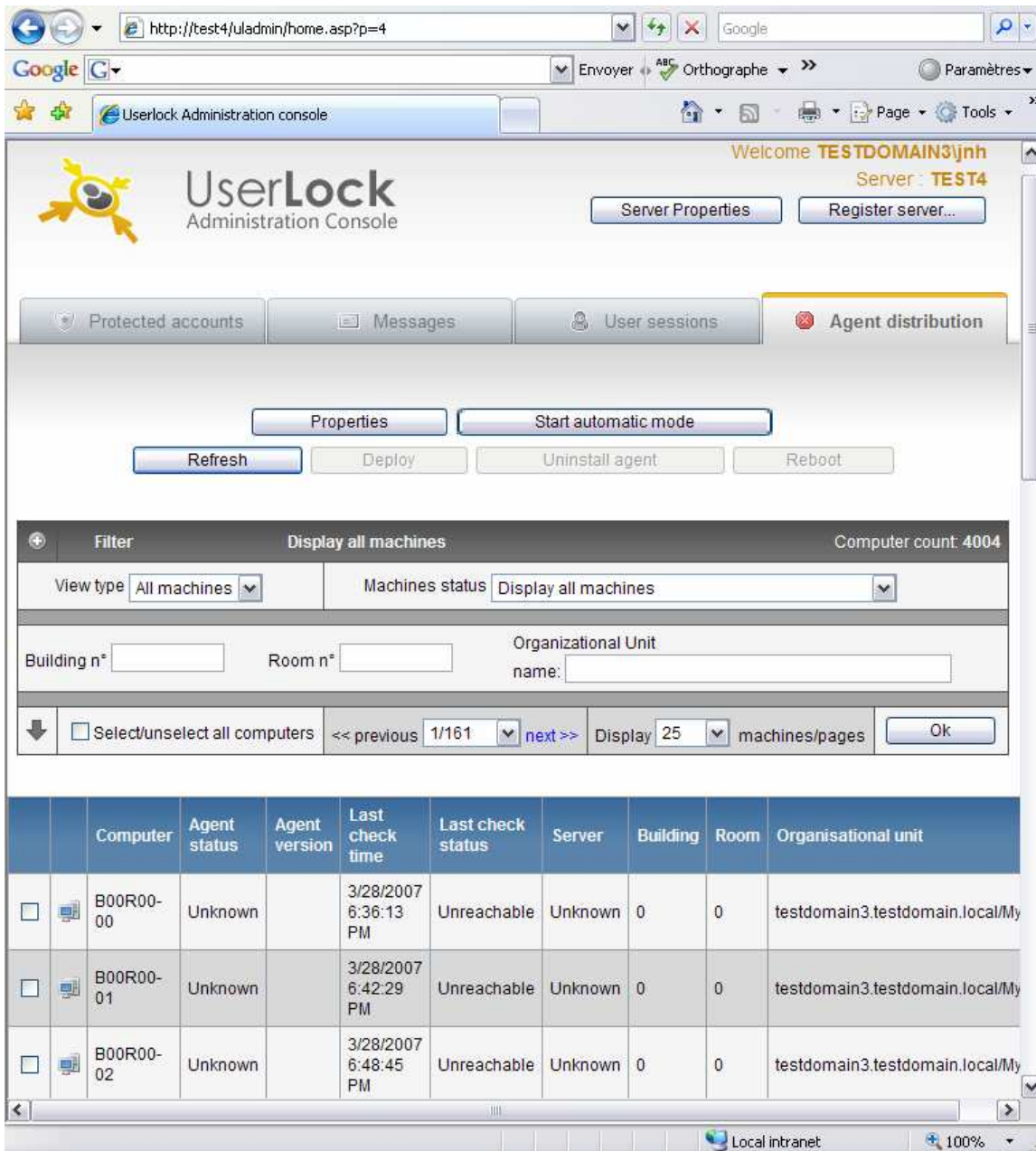


Figure 11 Agent distribution in the web console (the filter bar is expanded)

► Ability to display reports from the Web console

Reports can now be displayed from any computer using the web console. This feature needs Acrobat Reader installed on the client computer.

To do this, click on the *Report* button in *User sessions* or you can click on a user/computer in order to display the report of the corresponding session history since 30 days.

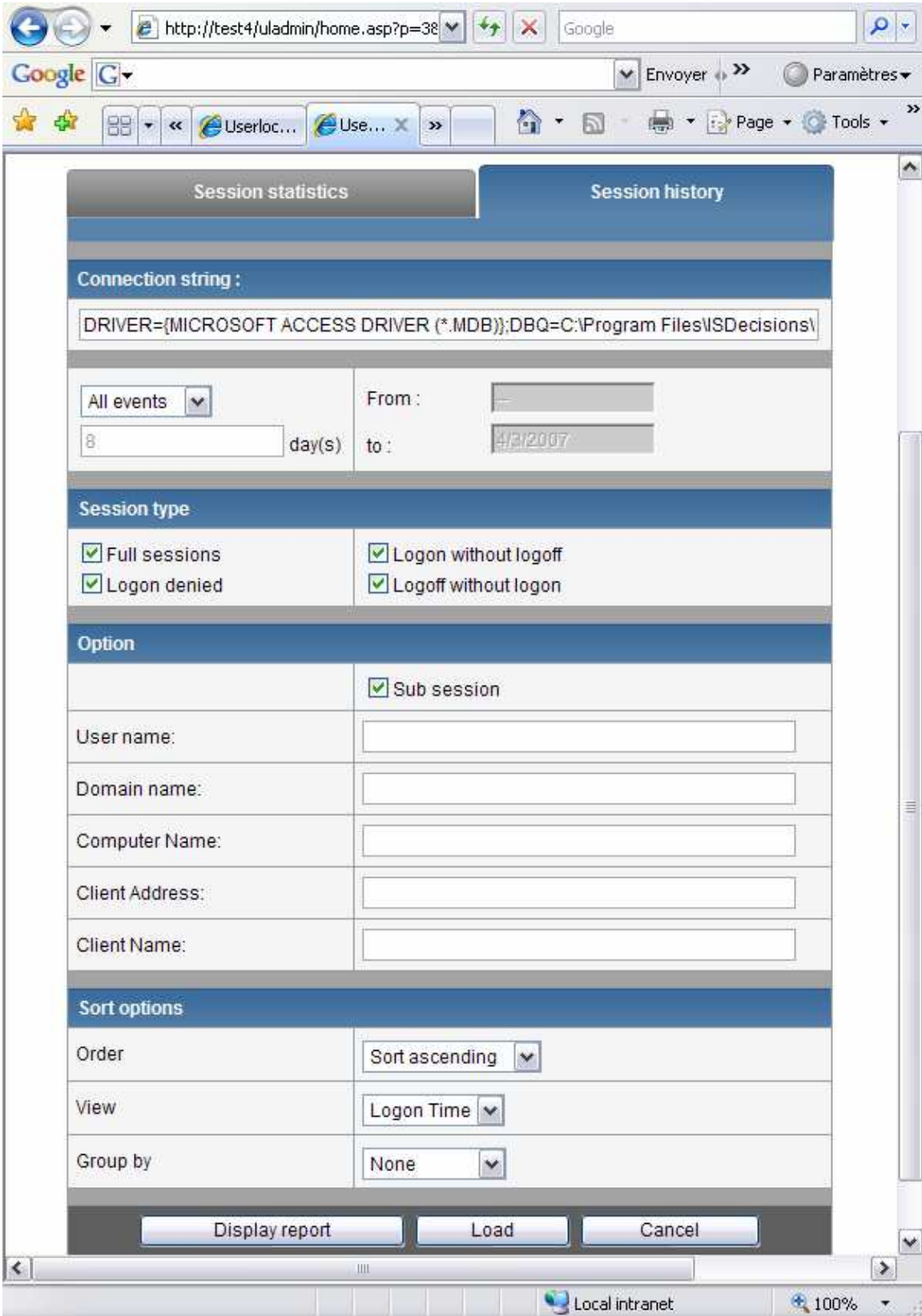


Figure 12 Report configuration in the web console

Syslocator

► Ability to enable a public Web interface to display system usage (per session status), allowing users to easily find an available computer; the interface can for example display systems available in a room (depending on computer naming convention), ideal for organizations with free access computers.

You can install the Syslocator on an IIS web site with the web configuration tool.

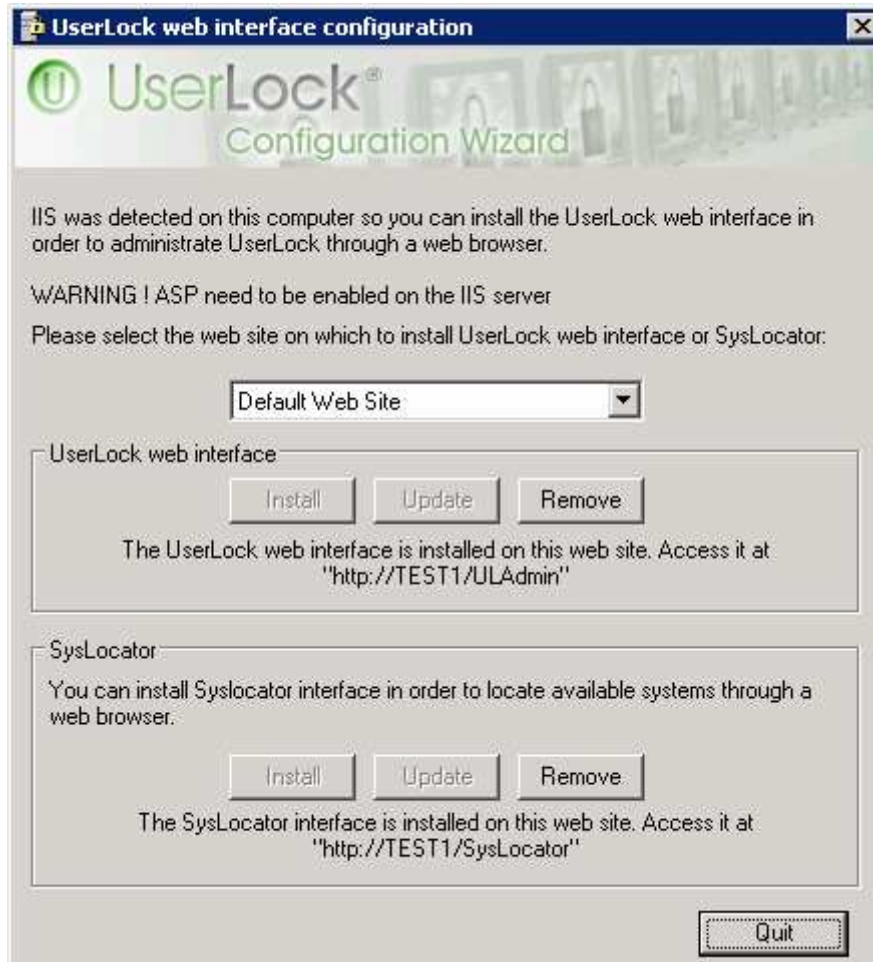


Figure 13 Configure the SysLocator on a IIS web site

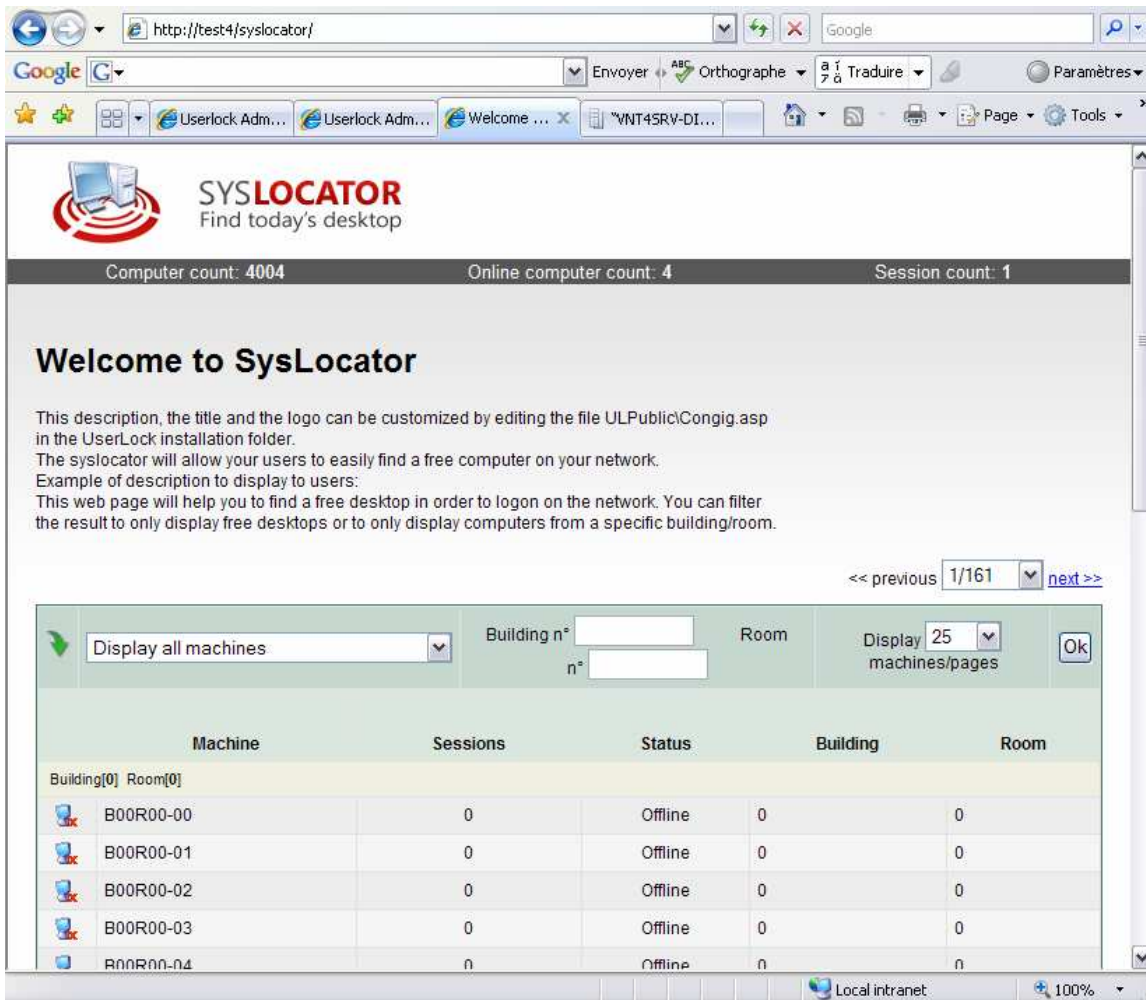


Figure 14 View of the SysLocator

The reporter

► Ability to automatically generate reports at regular intervals, to update for example a Web site or to email (using third party software).

When the report is configured, use the schedule button in the reporter (See below). Dates are saved relatively so the time frame will shift automatically with the date when the report is generated.

► Two new reports

These two new reports display a printable version of what you can see in the administration console. These reports query directly the UserLock server and don't use the database.
Agent Distribution: View of the agent installation status on all computers of the protected network zone.

User sessions: Instantaneous view of all user session at display time.

In order to avoid any misunderstanding the old "User sessions report" was renamed into "Session history".

The four reports are available in the new "UserLock Reporter".

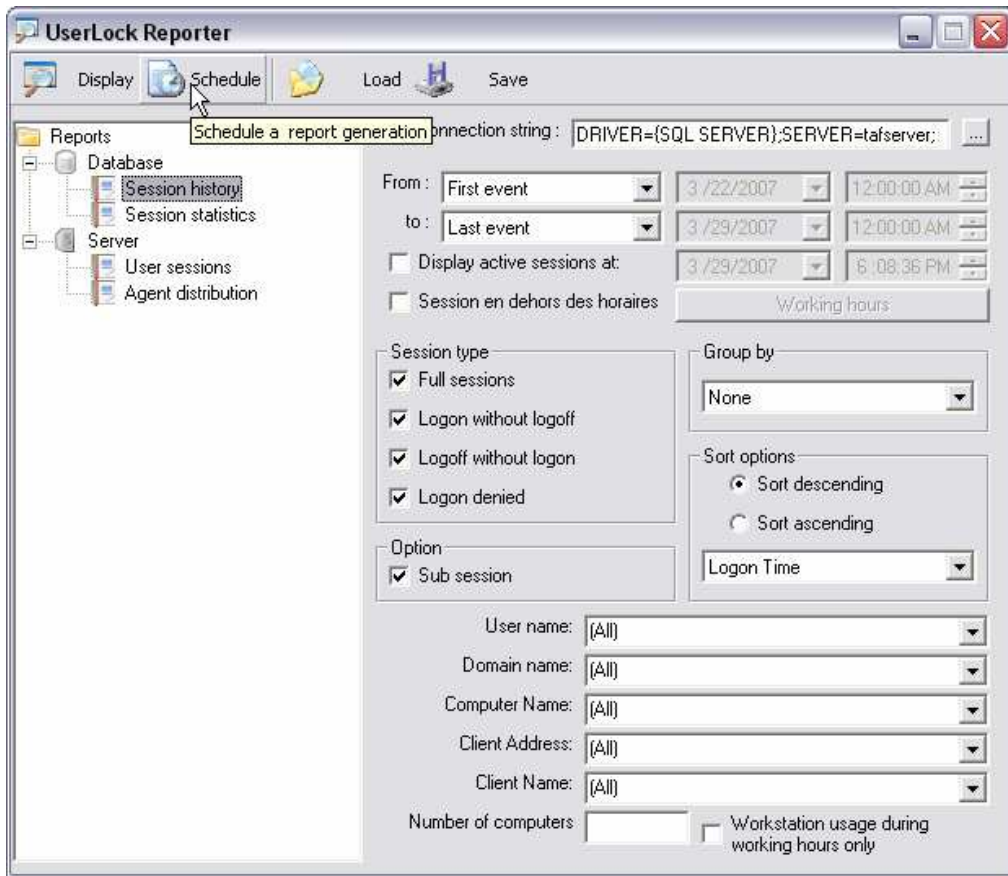


Figure 15 Configuration of the Session history report (formerly user sessions report) in the UserLock reporter

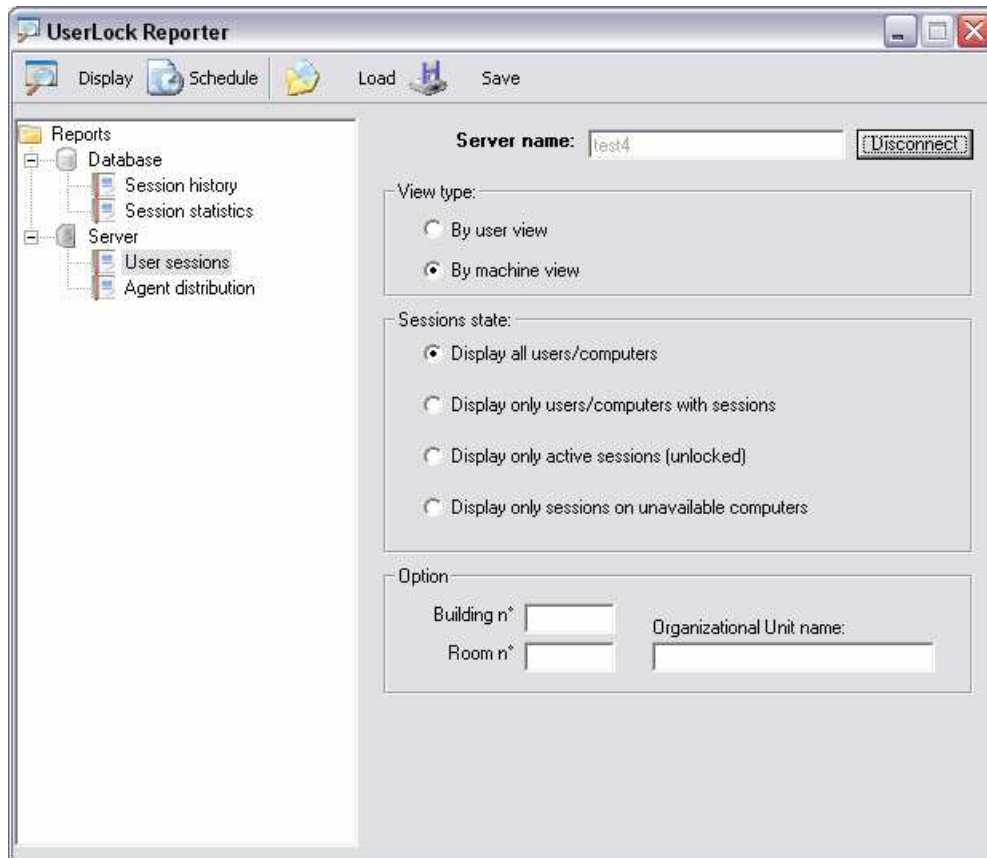


Figure 16 Configuration of the new User sessions report in the UserLock reporter

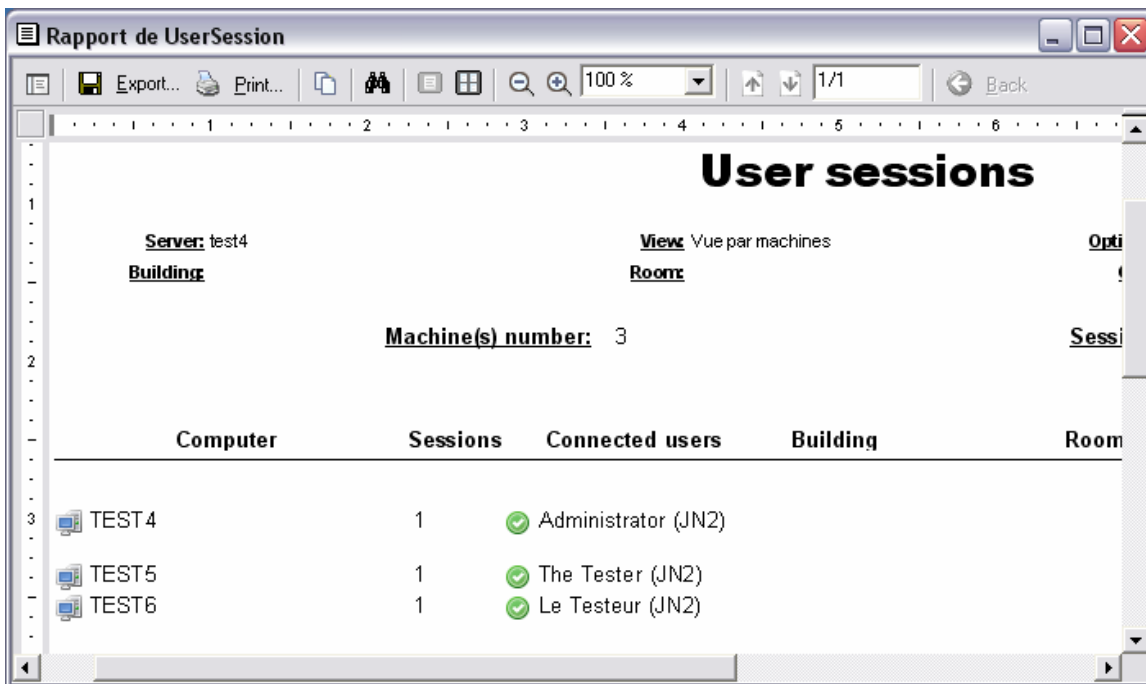


Figure 17 Result of the new User sessions report

Agent

▶ Improved UserLock agent

The agent will inform the UserLock server of its status at each startup. Currently it's the server that checks this at regular intervals, which slows down the display on the console.

The agent will detect computer crashes and send the crash time to the UserLock server upon computer reboot. This will improve session timing precision.

The agent will regularly send any unsent session events due to for example network problems at time of session startup.

▶ Support of Windows Vista

In Windows Vista Microsoft completely changed the logon process and the GINA technology was removed. In consequence a new agent is now needed to manage Windows Vista computers. The integrated deployer will automatically choose the version of the agent to install on a workstation according to the version of its operating system. The Windows Vista agent doesn't need a reboot of the workstation after the installation.

▶ Terminal session connection/disconnection tracking

In the previous version UserLock was only able to track lock/unlock events but terminal sessions can also be disconnected. This is equivalent to a session lock as the user no longer accesses the session. Now UserLock will track connection/disconnection events allowing to get precise session timing and to follow terminal changes after each reconnection.