

What's new in UserLock?

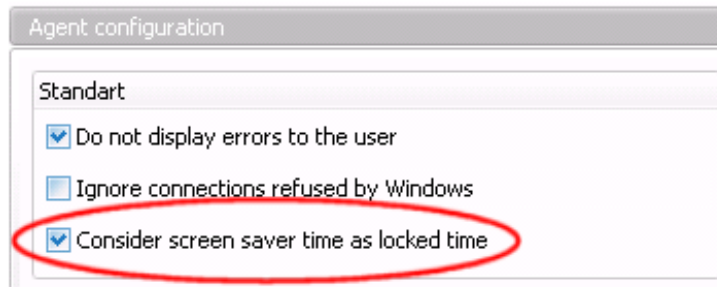
What's new in UserLock 5.5?	2
1.New Screen saver feature	2
2.New Idle Time feature	2
3.New Shut Down feature	3
4.New Group Policies feature	3
5.Improvements and optimizations	3
What's new in UserLock 5.0?	4
1.New interface	4
1.1.WINDOWS CONSOLE	4
1.2.WEB CONSOLE	9
2.Reports	10
2.1.GENERAL	10
2.2.HOW TO SCHEDULE A REPORT AND SEND IT AUTOMATICALLY BY MAIL	11
2.3.NEW MODE FOR THE SESSION STATISTICS REPORT.....	17
3.Ras sessions	18
3.1.VPN SESSIONS WITH A RRAS SERVER	19
3.2.RADIUS SESSIONS WITH IAS SERVER	19
3.3.CONFIGURING RESTRICTIONS FOR RAS SESSIONS	20

For additional information, please contact IS Decisions at one of the following:

What's new in UserLock 5.5?

1. New Screen Saver feature

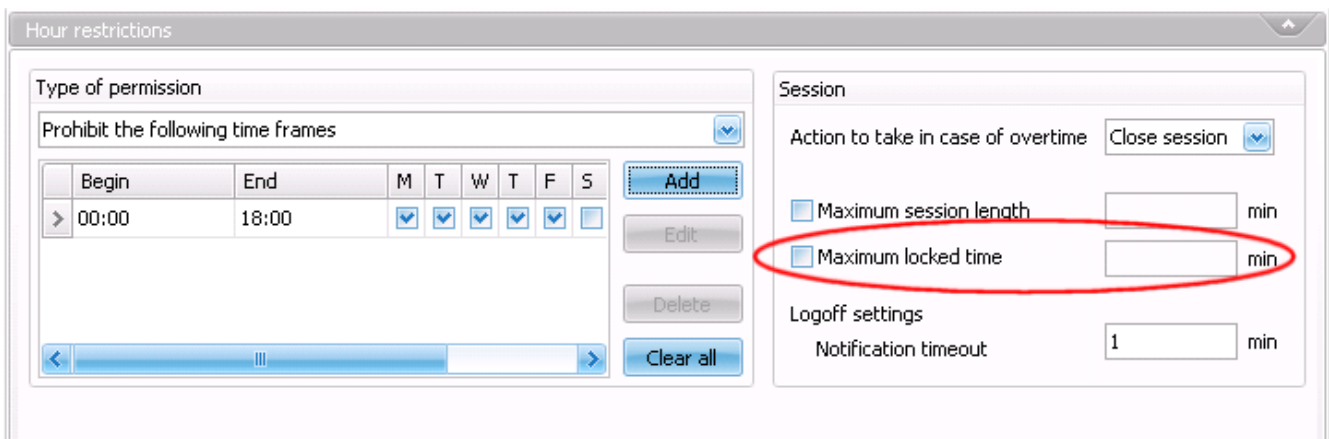
The agent can now send a lock notification when a password protected screensaver starts.



In *Agent distribution* properties select "Consider screen saver time as locked time".

2. New Idle Time feature

UserLock can now automatically logoff a session locked for longer than a specified time length. Combined with the ability to notify a lock event when screen saver starts, sessions can be closed after a specified time length of inactivity.



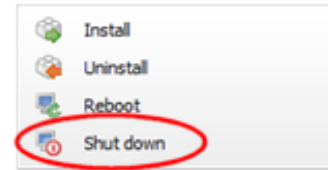
In *Protected accounts* select "Maximum locked time" and specify a number of minutes.

For additional information, please contact IS Decisions at one of the following:

3. New Shut Down feature

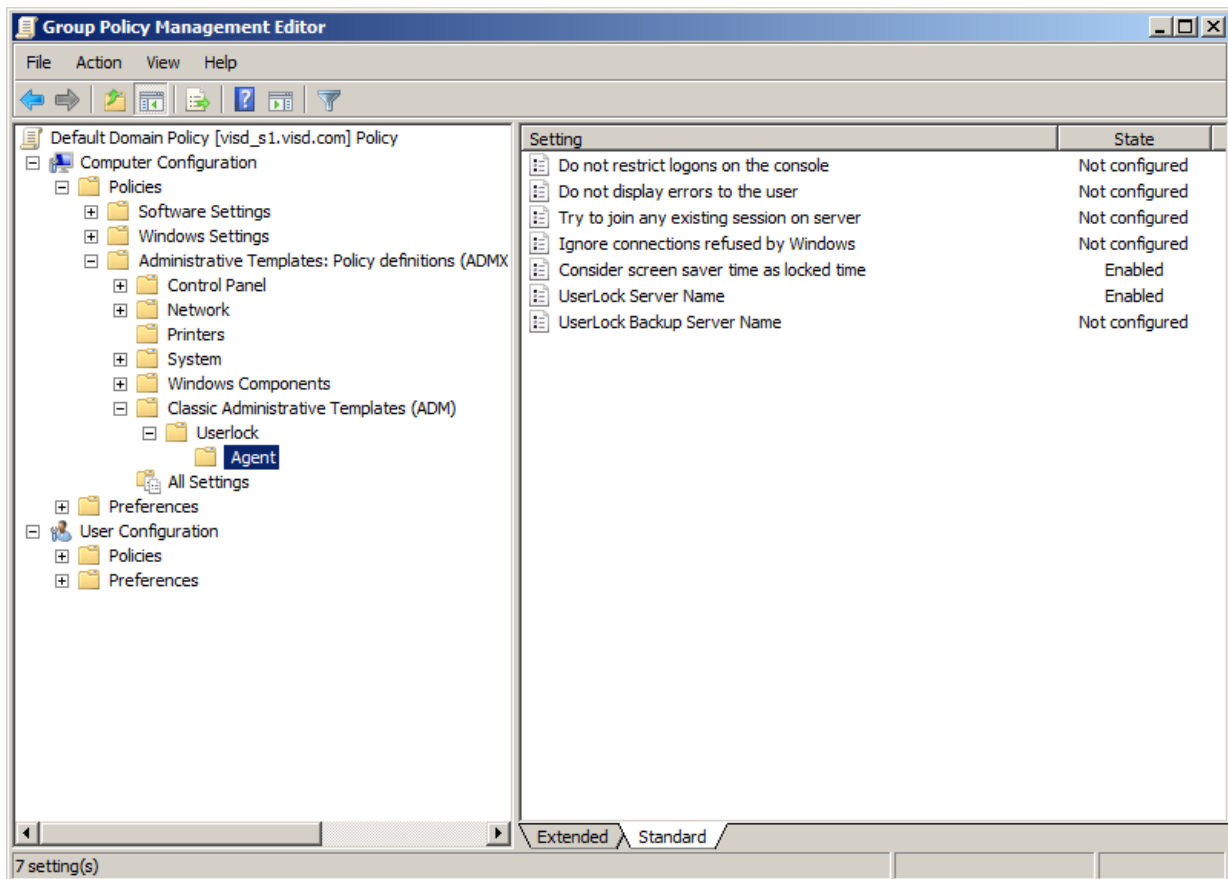
You can now power off computers from the UserLock console.

Perform a remote *Shut down* in *Agent Distribution* section using contextual menu or *Actions* tab after having selected computers.



4. New Group Policies feature

An *.adm* file is now available in the installation folder of UserLock. It allows deploying agent settings using *Group Policies*. This is useful if you already deployed the agent using the *MSI package* and *Group Policies*.



5. Improvements and optimizations

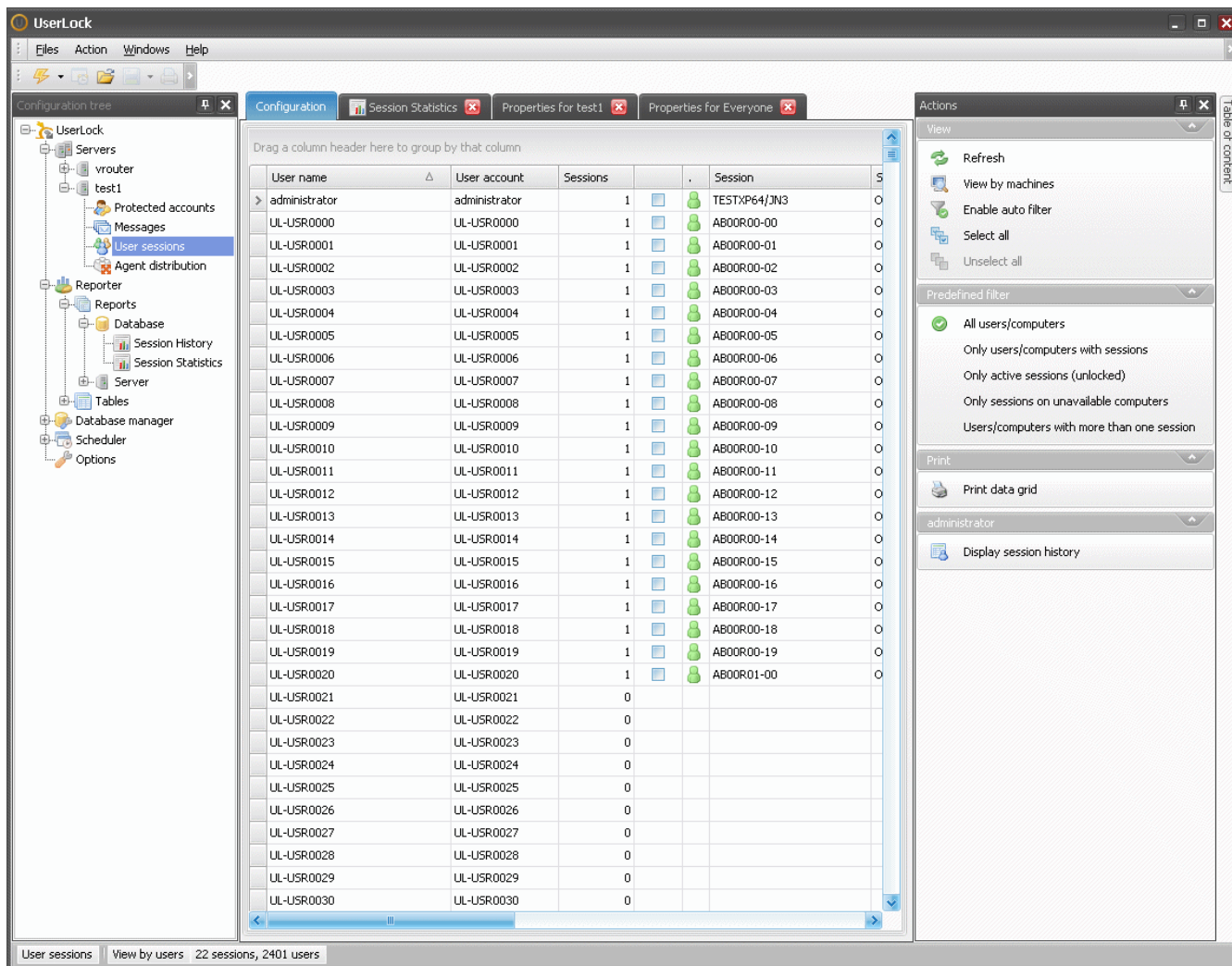
- Ability to use a large number of users *Protected account* (up to 10000).
- The query of the *Session history report* was optimized in order to display the report faster.
- The *Session history report* can now display independently *Logons denied by UserLock* and *Logons denied by Windows* (e.g. *Invalid password*).

For additional information, please contact IS Decisions at one of the following:

What's new in UserLock 5.0?

1. New interface

1.1. Windows console



- A brand new tabbed interface.
- A new **dashboard** allowing displaying statistics in charts.
- Reports are displayed in a new tab instead of a new window.
- New properties editor. Properties are displayed in a new tab instead of a new window.
- *Reporter* is integrated into the console.
- *Logon Cleaner* is integrated into the console.
- *Scheduler* is integrated into the console.
- **The generation of reports can easily be scheduled** without running command lines. Reports can also automatically be sent to an E-mail recipient (See *Reports* section).
- *Actions* you can perform using the context menu are also displayed in the **Actions Panel**.

For additional information, please contact IS Decisions at one of the following:

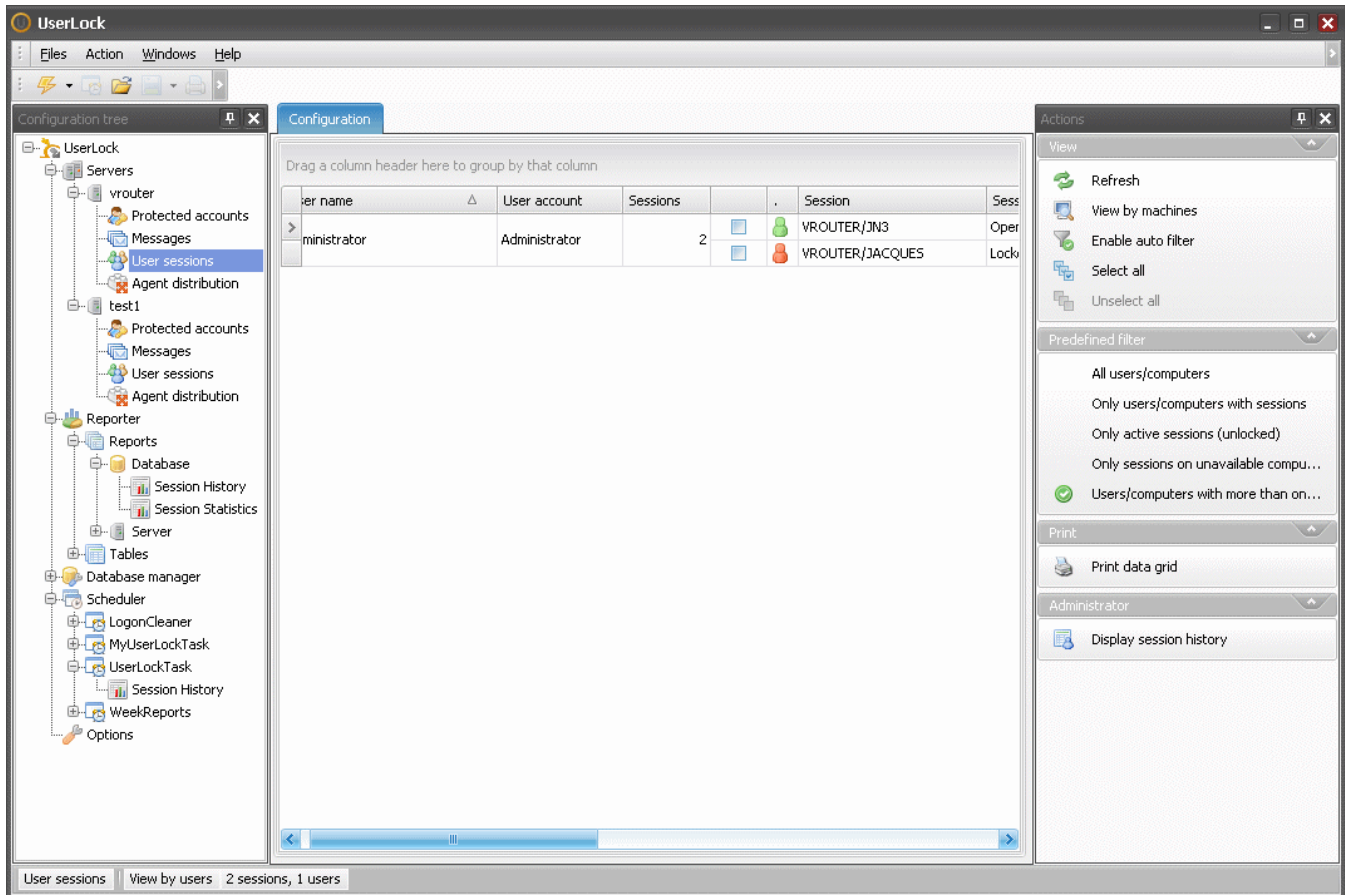
- The **Active Directory Tree** can be displayed for the *Agent distribution* view and the *User sessions View by machines*.

The screenshot displays the UserLock application window. On the left is a navigation pane with a tree structure. The main area is divided into several panes:

- Configuration tree:** Shows a hierarchy starting with 'UserLock', then 'Servers', 'test1', 'Protected accounts', 'Messages', 'User sessions', and 'Agent distribution' (selected).
- Active Directory tree:** Shows a hierarchy starting with 'testdomain.local', then 'Computers' (selected), and a list of computers including 'Domain Controllers', 'MyOu', 'testdomain3.testdo...', 'MyUnit', and 'RealComputers'.
- Table:** A table with columns: Computer, Agent type, Agent status, and Agent version. It lists 24 computers, all with 'Desktop' agent type and 'Unknown' status. The status bar at the bottom indicates '1 installed agents, 8013 computers'.
- Actions pane:** Contains sections for 'Agent distribution' (Start Automatic mode, Properties), 'View' (Refresh, Hide AD tree, Enable auto filter, Select all, Unselect all), 'Predefined filter' (Display all machines, Display only DC, Display only machines without the agent ins..., Display only unavailable machines), and 'Print' (Print data grid).

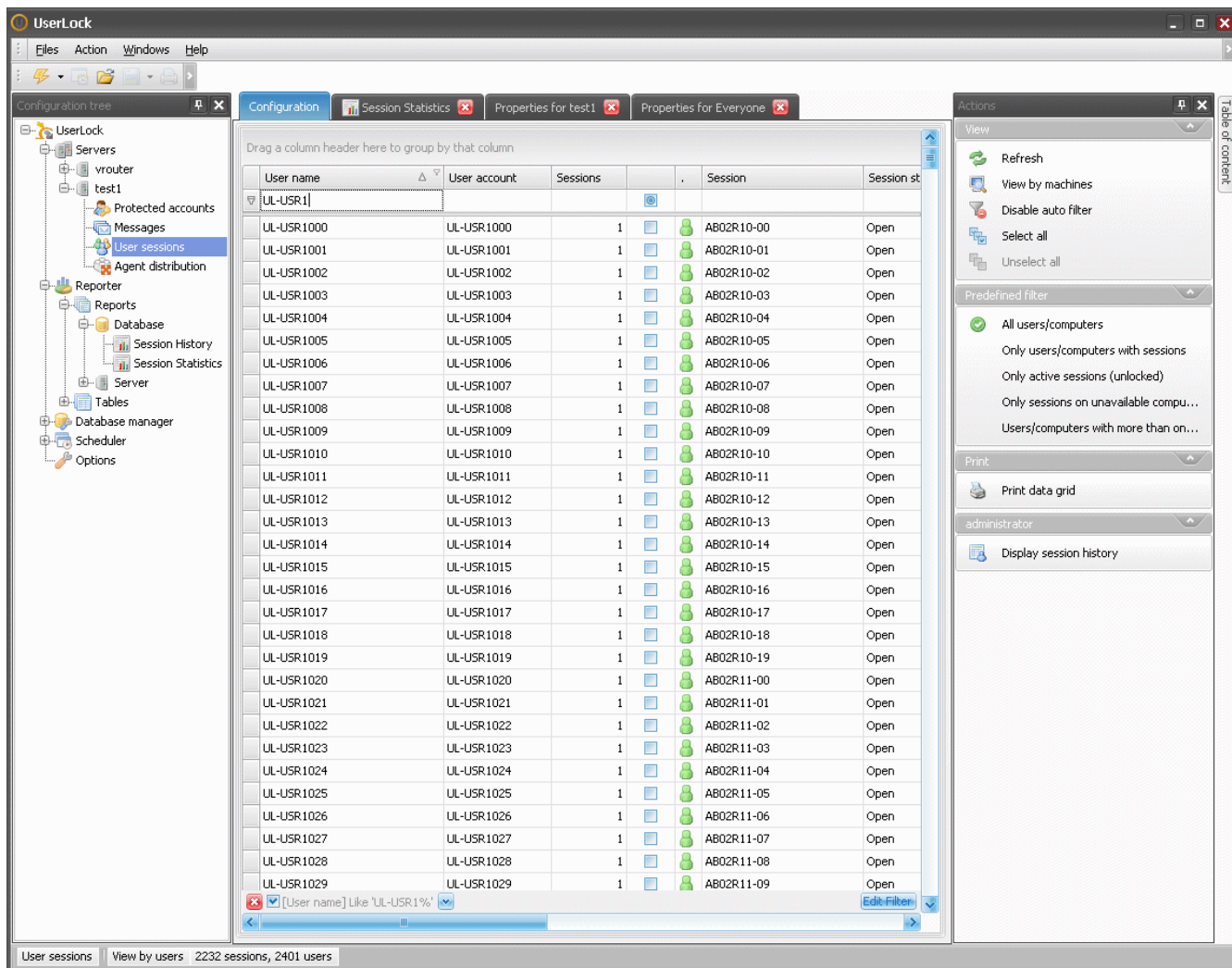
For additional information, please contact IS Decisions at one of the following:

- A **new predefined filter** has been added allowing to only displaying users or computers with more than one session.



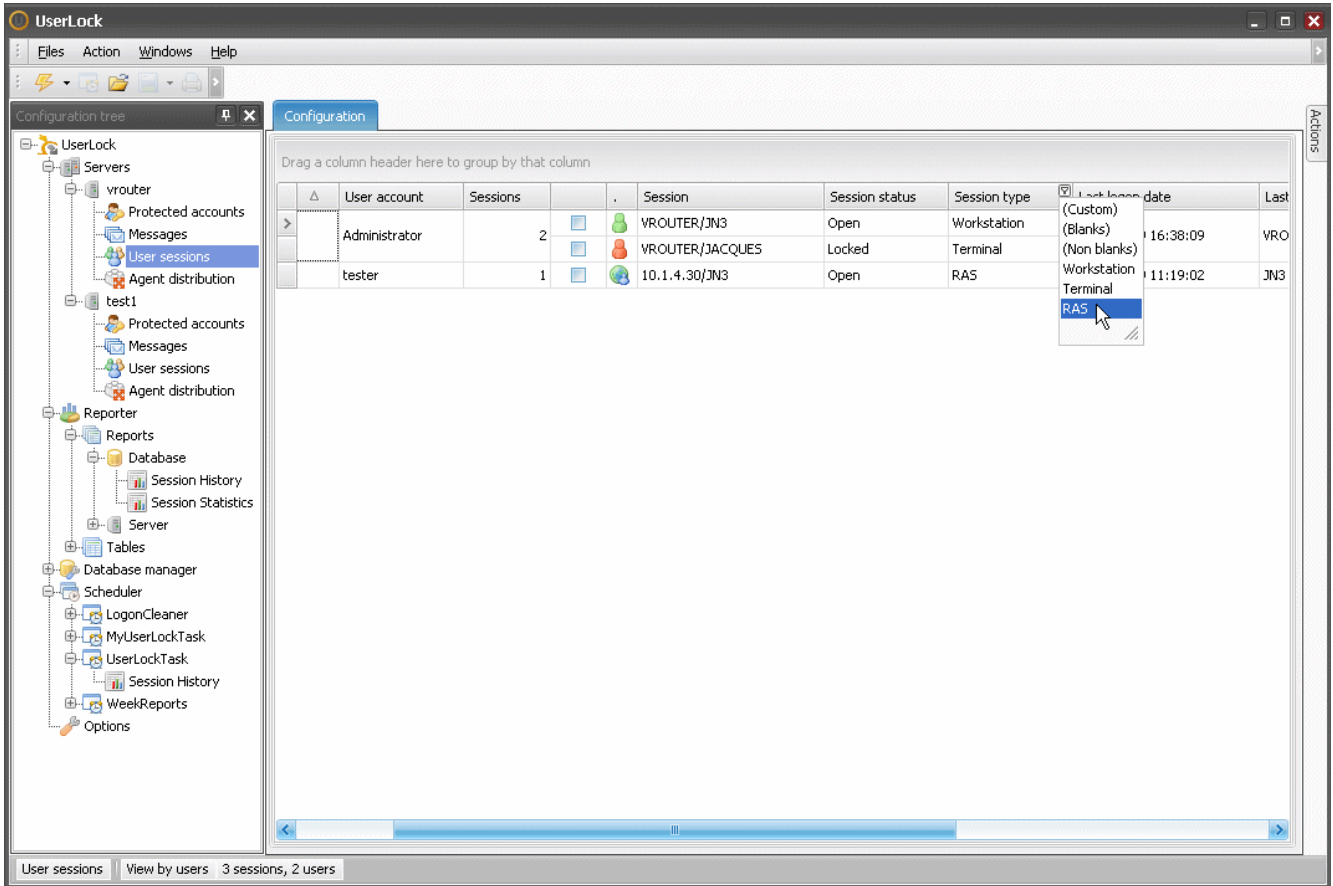
For additional information, please contact IS Decisions at one of the following:

- **Auto filter** to quickly find users or computers in the console (Click on *Enable auto filter* in the Actions Panel).

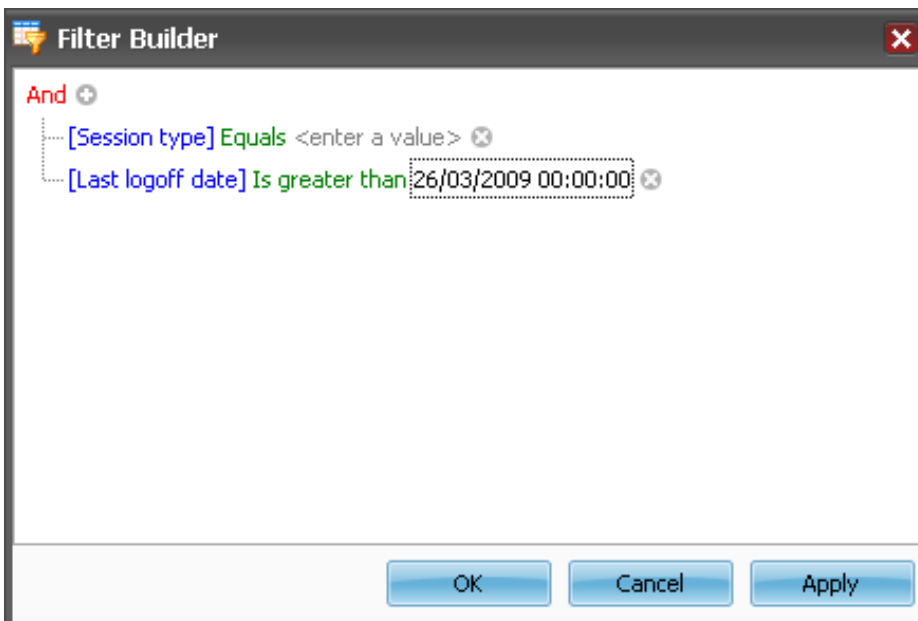


For additional information, please contact IS Decisions at one of the following:

- **Quick filter:** You can click on the right top corner of a column header in order to display the list of all values in the column. Select a value in order to filter the view on the selected column and value.



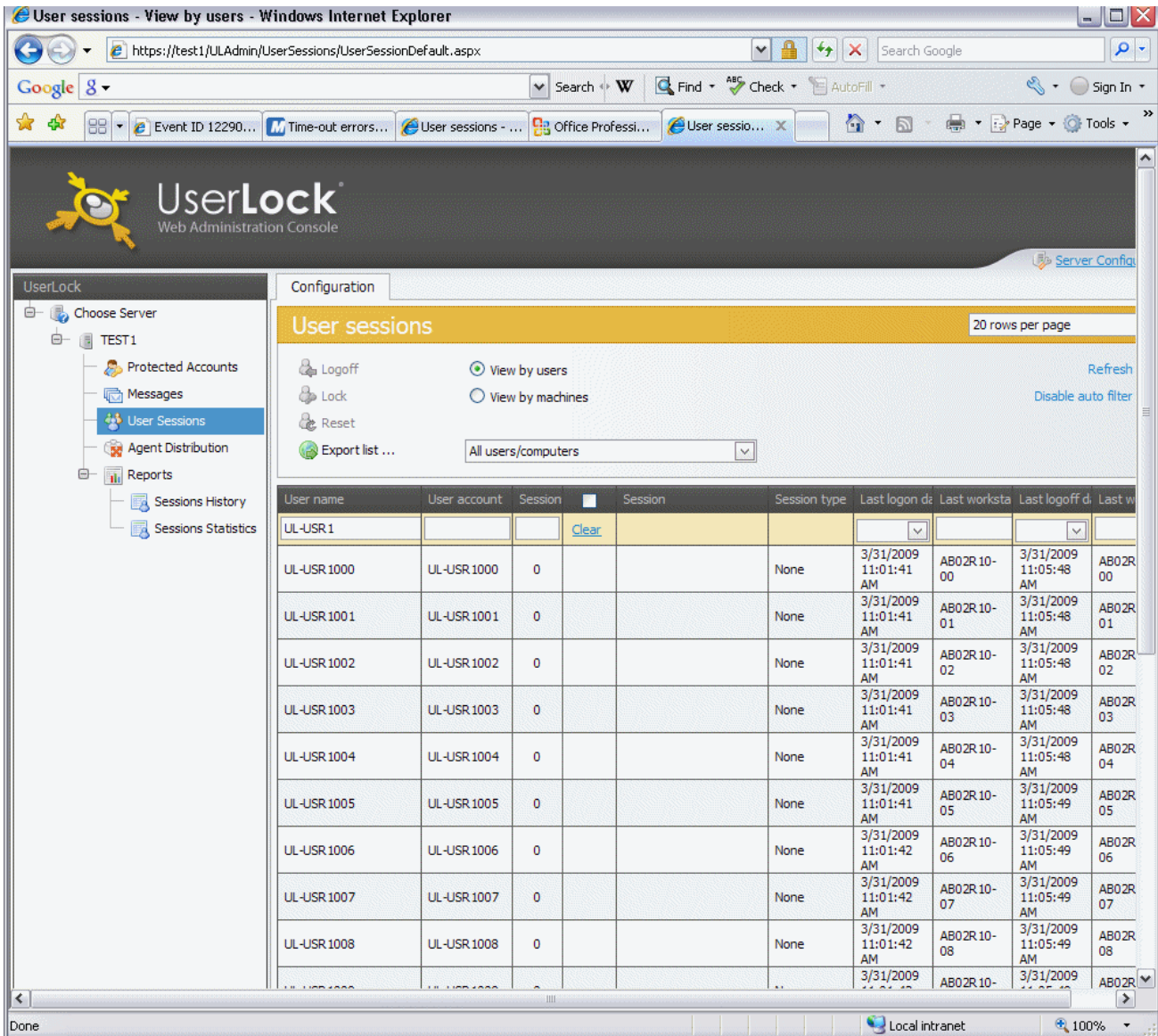
- You can also configure an **Advanced filter**. Right click on a column header and click on *Filter Editor*.



For additional information, please contact IS Decisions at one of the following:

1.2. Web console

- A brand **new** interface.
- A new **dashboard** allowing displaying statistics in charts.
- **Ability to sort users and computers** according to a specific row. Just click on the row header.
- **Auto Filter** to quickly find users or computers in the console.
- The **Active Directory Tree** can be displayed for the *Agent distribution view* and the *User sessions View by machines*.
- UserLock access rights are now available in the Web console using *Server properties*.
- The *User sessions* view now displays user's full name and account's name.



User sessions - View by users - Windows Internet Explorer

https://test1/ULAdmin/UserSessions/UserSessionDefault.aspx

UserLock
Web Administration Console

Configuration

User sessions 20 rows per page

Logoff View by users Refresh
 Lock View by machines Disable auto filter
 Reset
 Export list ... All users/computers

User name	User account	Session	Session	Session type	Last logon date	Last worksta	Last logoff date	Last w
UL-USR 1			Clear					
UL-USR 1000	UL-USR 1000	0		None	3/31/2009 11:01:41 AM	AB02R 10-00	3/31/2009 11:05:48 AM	AB02R 00
UL-USR 1001	UL-USR 1001	0		None	3/31/2009 11:01:41 AM	AB02R 10-01	3/31/2009 11:05:48 AM	AB02R 01
UL-USR 1002	UL-USR 1002	0		None	3/31/2009 11:01:41 AM	AB02R 10-02	3/31/2009 11:05:48 AM	AB02R 02
UL-USR 1003	UL-USR 1003	0		None	3/31/2009 11:01:41 AM	AB02R 10-03	3/31/2009 11:05:48 AM	AB02R 03
UL-USR 1004	UL-USR 1004	0		None	3/31/2009 11:01:41 AM	AB02R 10-04	3/31/2009 11:05:48 AM	AB02R 04
UL-USR 1005	UL-USR 1005	0		None	3/31/2009 11:01:41 AM	AB02R 10-05	3/31/2009 11:05:49 AM	AB02R 05
UL-USR 1006	UL-USR 1006	0		None	3/31/2009 11:01:42 AM	AB02R 10-06	3/31/2009 11:05:49 AM	AB02R 06
UL-USR 1007	UL-USR 1007	0		None	3/31/2009 11:01:42 AM	AB02R 10-07	3/31/2009 11:05:49 AM	AB02R 07
UL-USR 1008	UL-USR 1008	0		None	3/31/2009 11:01:42 AM	AB02R 10-08	3/31/2009 11:05:49 AM	AB02R 08

For additional information, please contact IS Decisions at one of the following:

2. Reports

2.1. General

- In order to display a report, select it in the tree, configure it and click on the *Launch* button in the toolbar.
- UserLock reports now use a new report engine and a new report design.

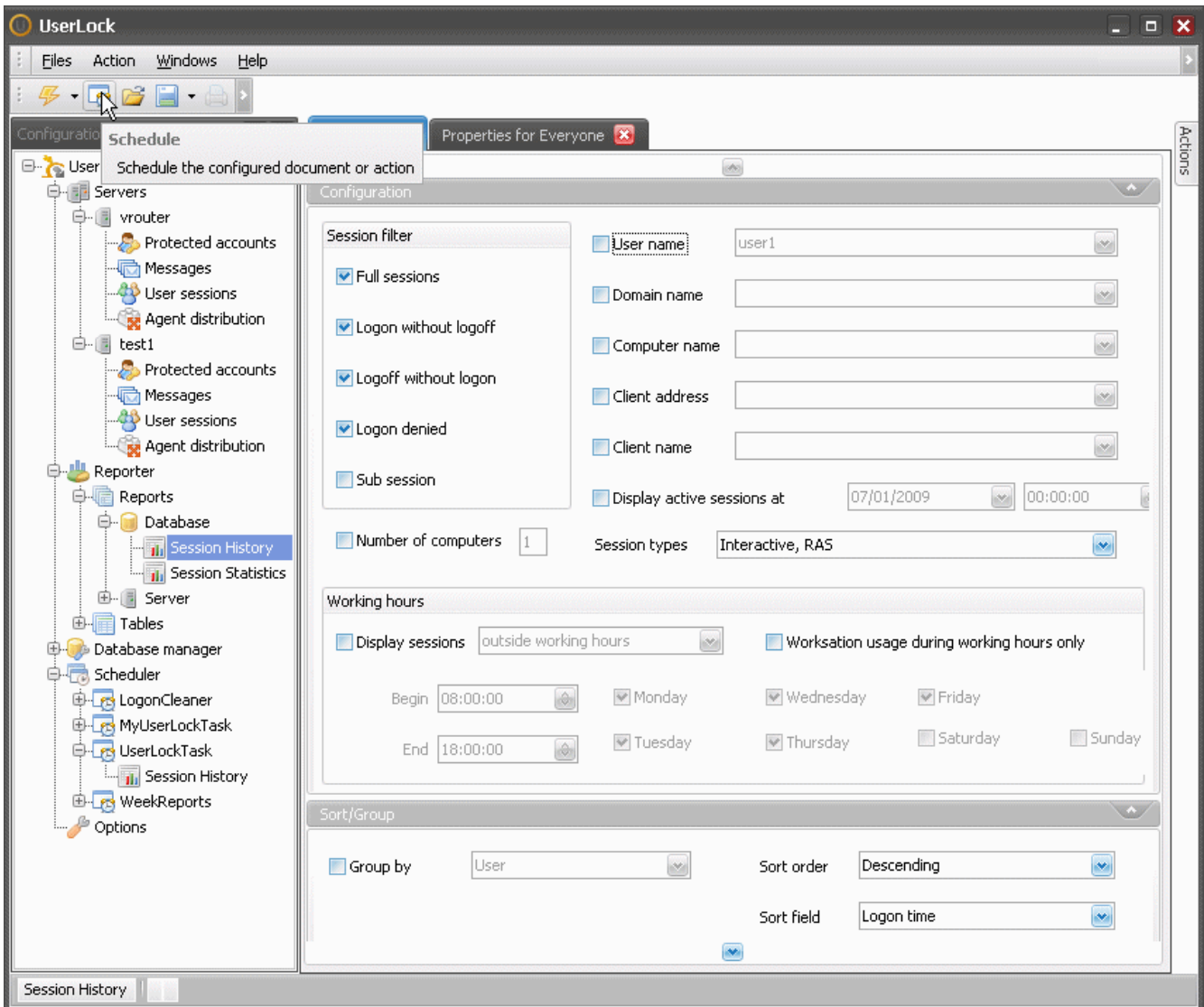
The screenshot shows the UserLock application window. On the left is a configuration tree with categories like Servers, Reporter, Database, and Tables. The 'Session History' report is selected. The main area displays the report configuration for 'UserLock Session History' dated 31/03/2009. Below the configuration is a table of session events.

Logon time	Logoff time	User	Domain	Comput
26/02/2004 17:26:48	--	user4	MYDOMAIN	WORKSTATION05
26/02/2004 16:20:28	--	user8	MYDOMAIN	WORKSTATION07
26/02/2004 14:37:18	26/02/2004 17:45:30	user6	MYDOMAIN	WORKSTATION03
26/02/2004 09:26:12	26/02/2004 18:28:58	user7	MYDOMAIN	WORKSTATION01
26/02/2004 09:19:36	--	user2	MYDOMAIN	WORKSTATION08
26/02/2004 09:15:15	26/02/2004 14:35:57	user6	MYDOMAIN	WORKSTATION03
26/02/2004 09:02:35	26/02/2004 17:15:41	user1	MYDOMAIN	WORKSTATION06
25/02/2004 17:43:07	25/02/2004 18:28:15	user8	MYDOMAIN	WORKSTATION07
25/02/2004 09:13:16	25/02/2004 17:07:28	user1	MYDOMAIN	WORKSTATION06
25/02/2004 09:12:27	25/02/2004 18:01:16	user6	MYDOMAIN	WORKSTATION03
25/02/2004 09:07:48	26/02/2004 17:43:52	user5	MYDOMAIN	WORKSTATION04

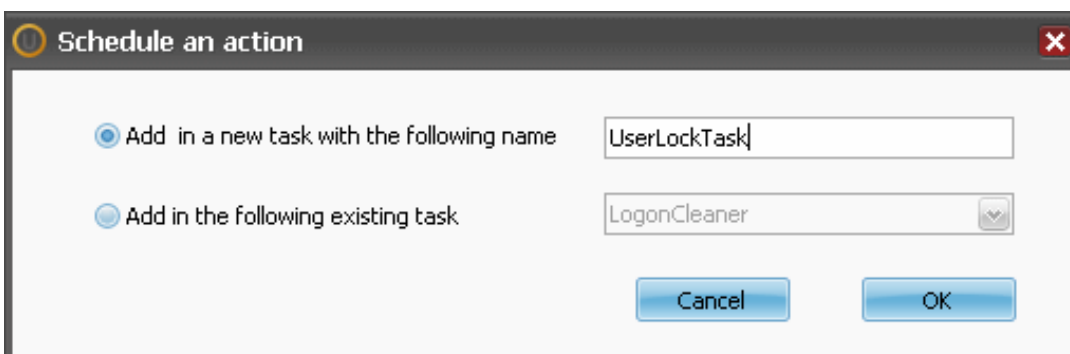
For additional information, please contact IS Decisions at one of the following:

2.2. How to schedule a report and send it automatically by mail

Configure the report and click on the *Schedule* button:

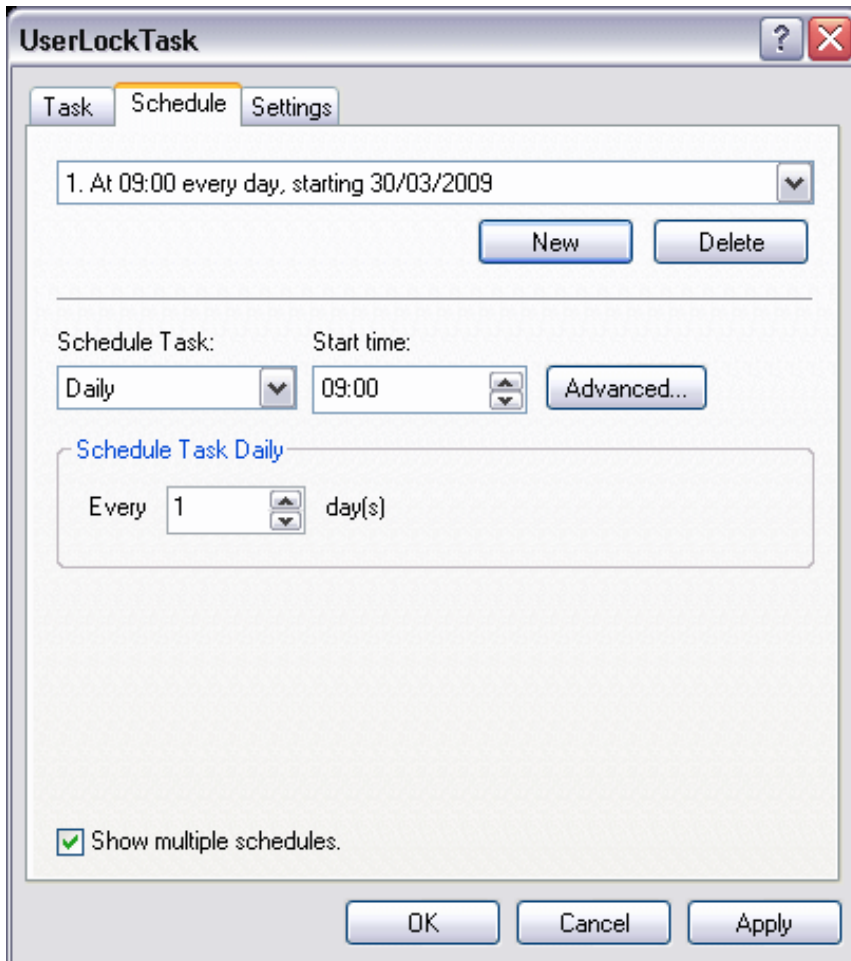


Type in a name for the new task:



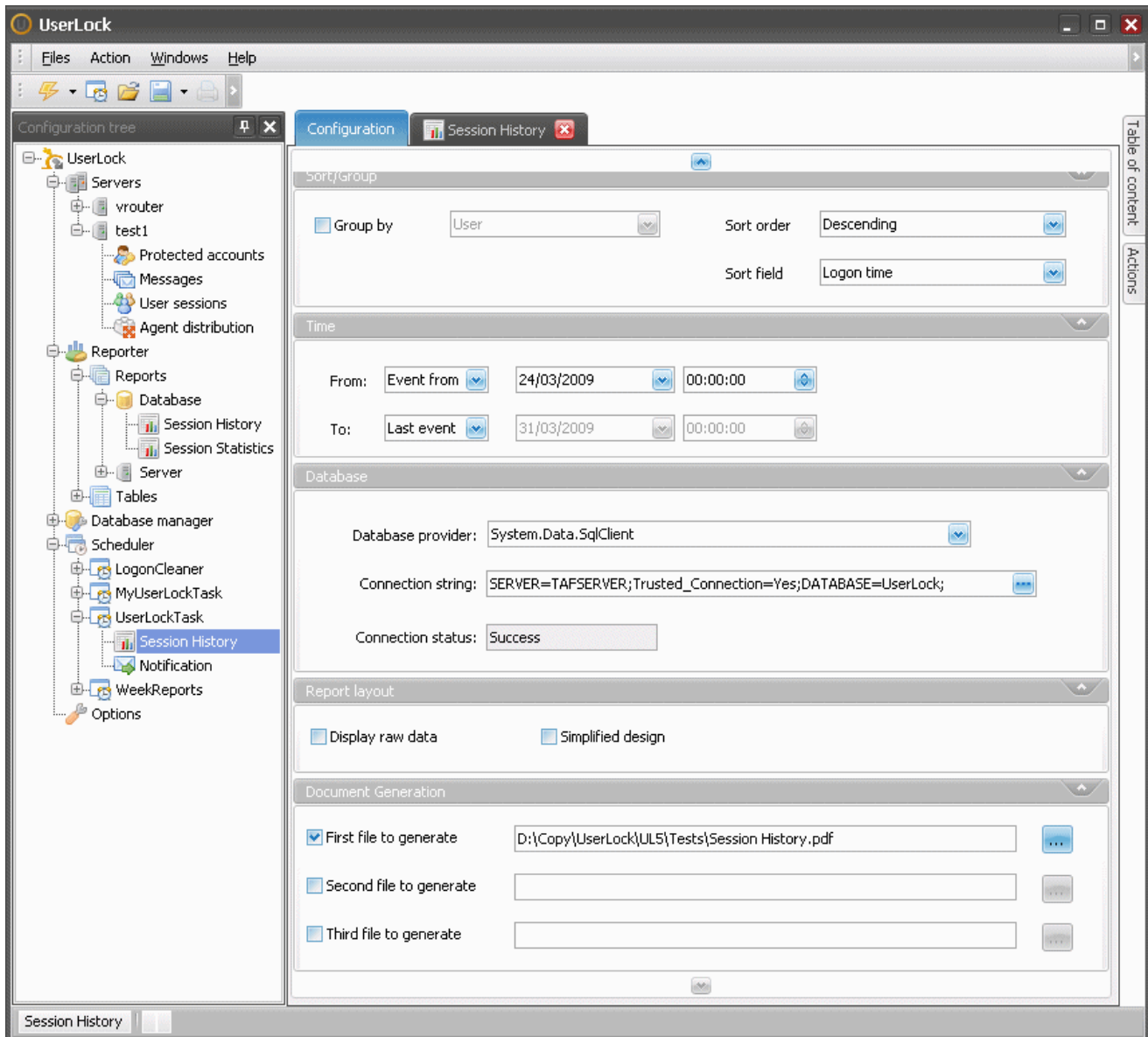
For additional information, please contact IS Decisions at one of the following:

Configure the *Schedule* tab:



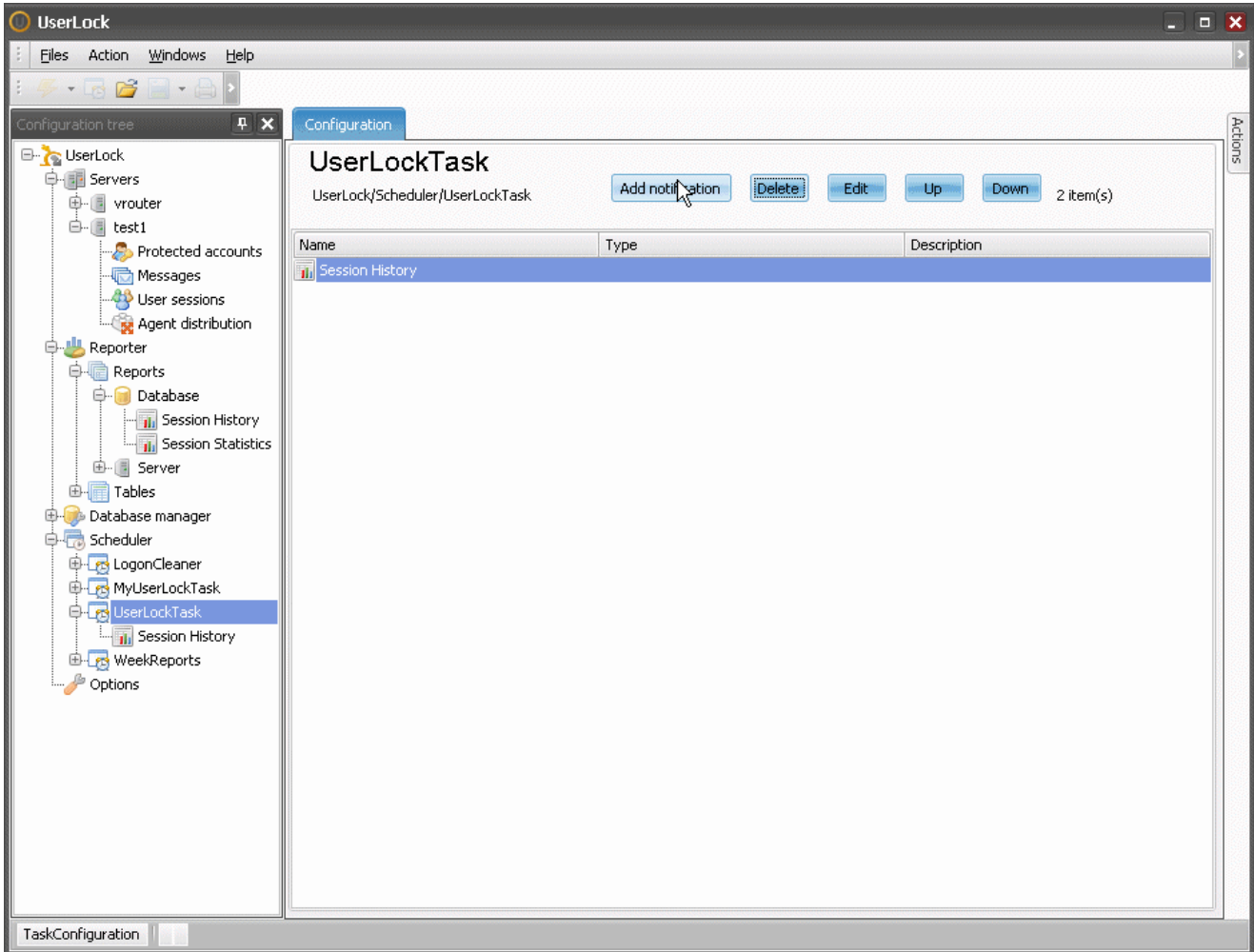
For additional information, please contact IS Decisions at one of the following:

The task is added into the *Scheduler* and you need to configure the file to generate a report:



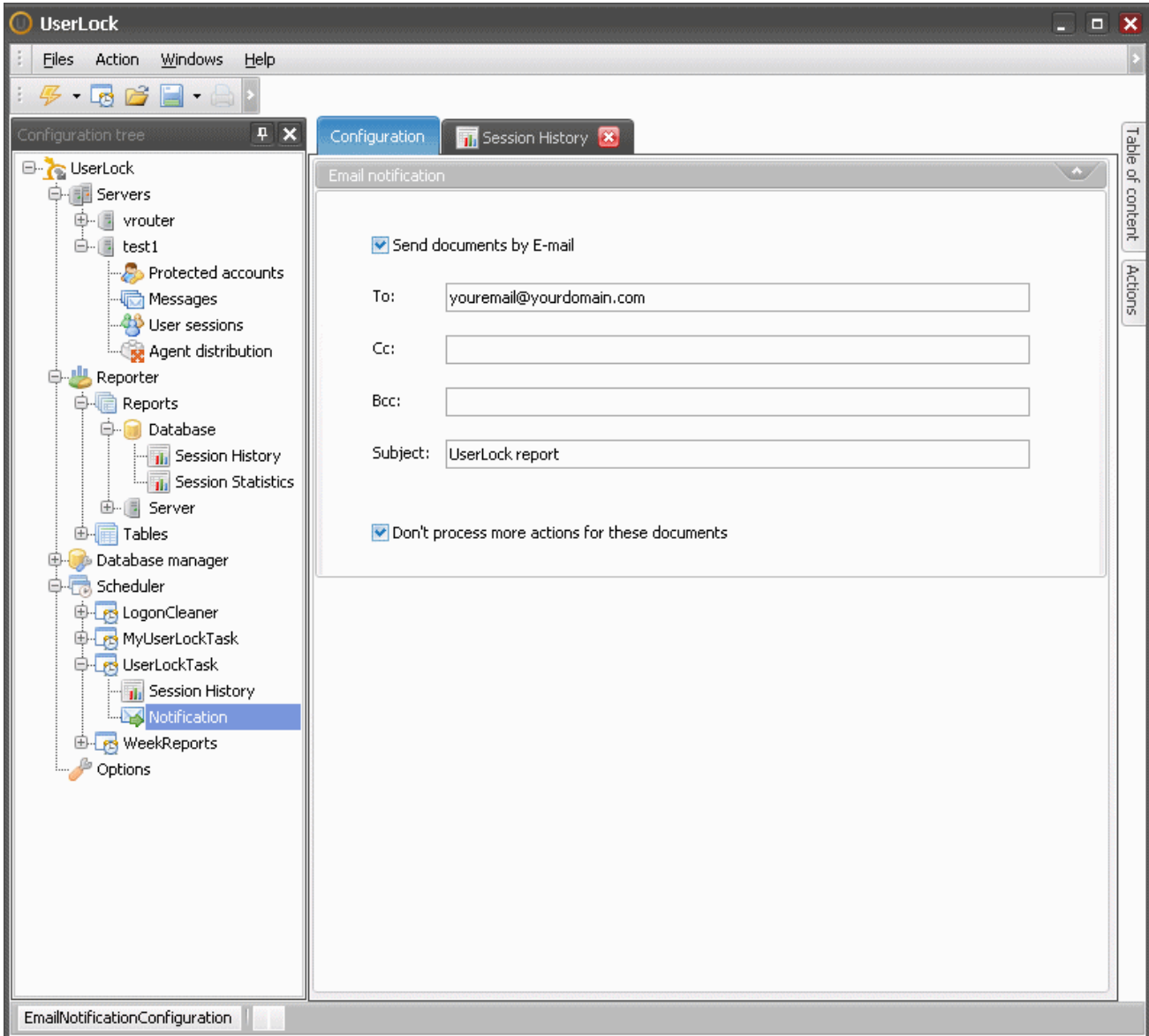
For additional information, please contact IS Decisions at one of the following:

Add a *Notification* action for the task to send the report by E-mail:



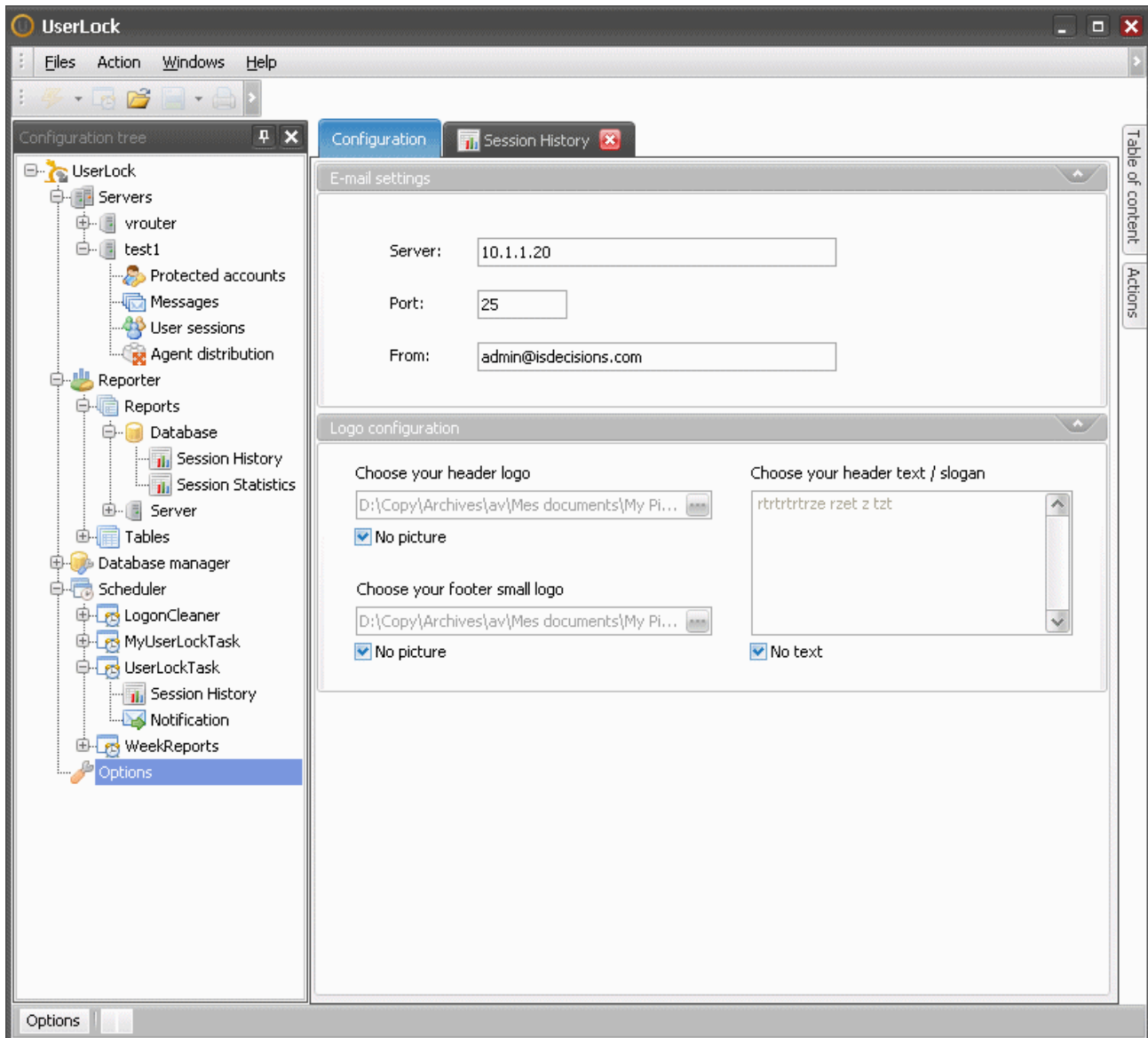
For additional information, please contact IS Decisions at one of the following:

Configure the *Notification*:



For additional information, please contact IS Decisions at one of the following:

Configure UserLock console SMTP settings (different from UserLock server SMTP settings):

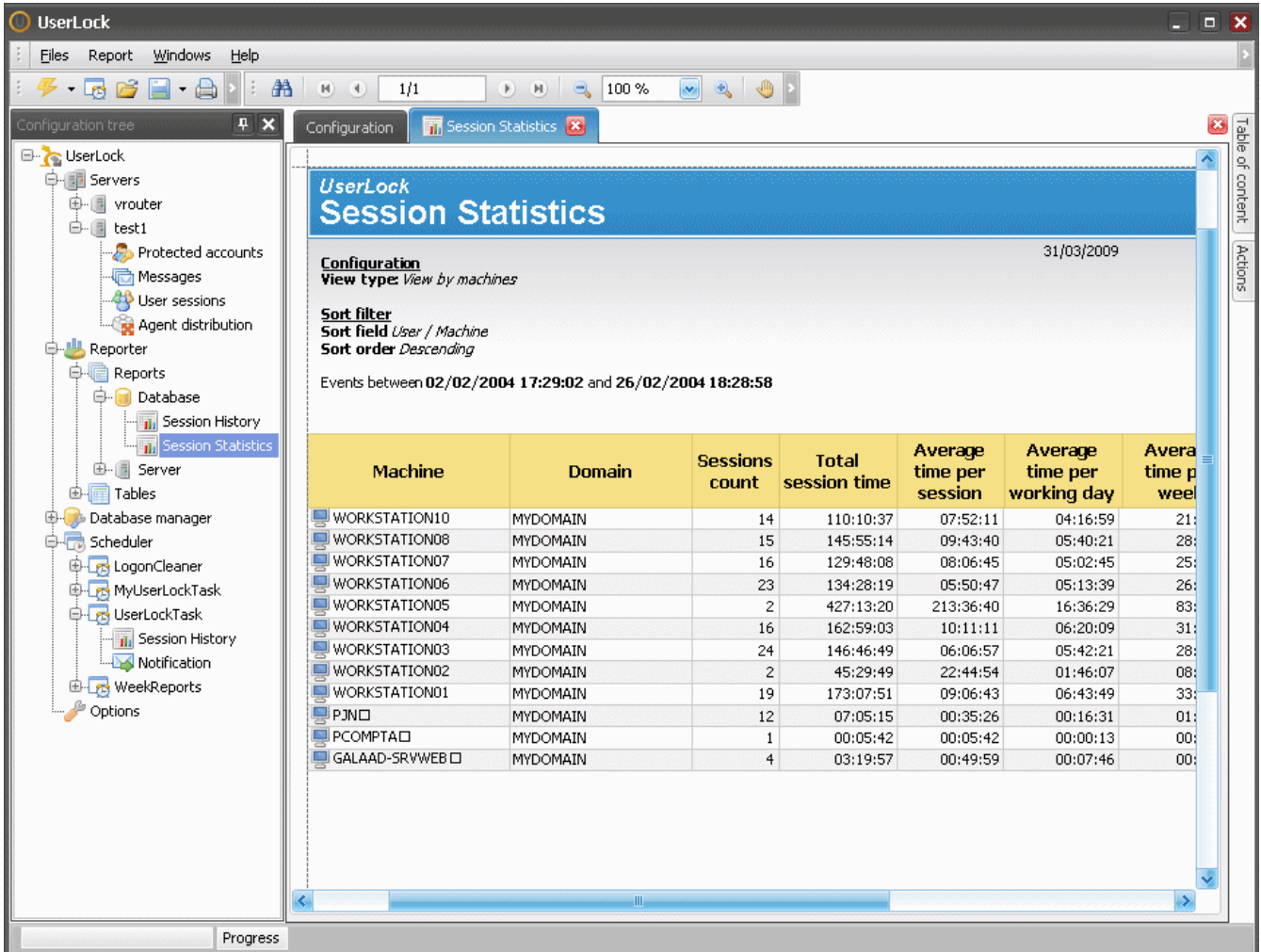


The report is now scheduled. Just wait for the scheduled time to automatically get the report in your mailbox.

For additional information, please contact IS Decisions at one of the following:

2.3. New mode for the Session statistics report

In previous UserLock versions, you already could display statistics about users. You can now also display statistics about computers.



UserLock Session Statistics
31/03/2009

Configuration
View type: View by machines

Sort filter
Sort field: User / Machine
Sort order: Descending

Events between 02/02/2004 17:29:02 and 26/02/2004 18:28:58

Machine	Domain	Sessions count	Total session time	Average time per session	Average time per working day	Average time per week
WORKSTATION10	MYDOMAIN	14	110:10:37	07:52:11	04:16:59	21:
WORKSTATION08	MYDOMAIN	15	145:55:14	09:43:40	05:40:21	28:
WORKSTATION07	MYDOMAIN	16	129:48:08	08:06:45	05:02:45	25:
WORKSTATION06	MYDOMAIN	23	134:28:19	05:50:47	05:13:39	26:
WORKSTATION05	MYDOMAIN	2	427:13:20	213:36:40	16:36:29	83:
WORKSTATION04	MYDOMAIN	16	162:59:03	10:11:11	06:20:09	31:
WORKSTATION03	MYDOMAIN	24	146:46:49	06:06:57	05:42:21	28:
WORKSTATION02	MYDOMAIN	2	45:29:49	22:44:54	01:46:07	08:
WORKSTATION01	MYDOMAIN	19	173:07:51	09:06:43	06:43:49	33:
PJN□	MYDOMAIN	12	07:05:15	00:35:26	00:16:31	01:
PCOMPTA□	MYDOMAIN	1	00:05:42	00:05:42	00:00:13	00:
GALAAD-SRWWEB□	MYDOMAIN	4	03:19:57	00:49:59	00:07:46	00:

For additional information, please contact IS Decisions at one of the following:

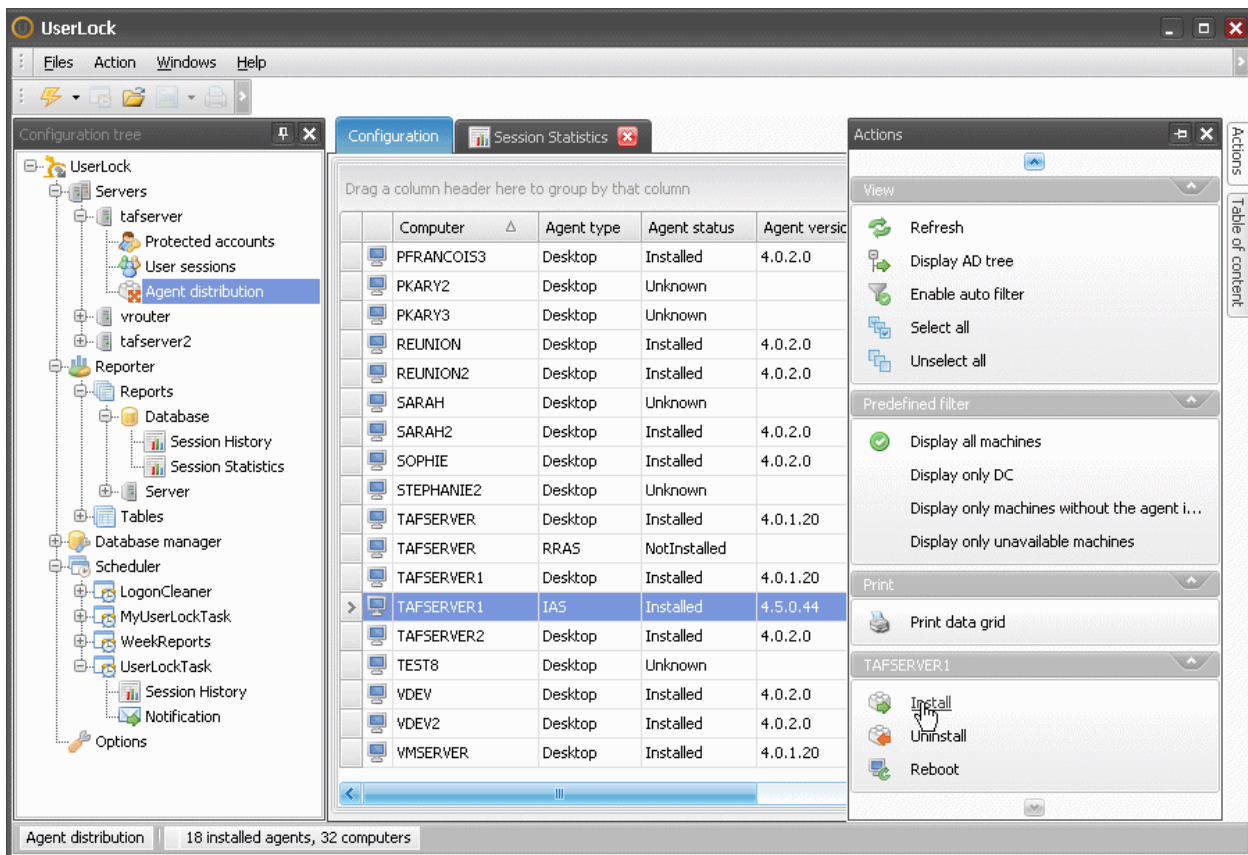
3. RAS sessions

UserLock 5 can protect RAS sessions on Microsoft RRAS (Routing and Remote Access Service) server or with any hardware router configured to authenticate users with RADIUS protocol on a Microsoft IAS (Internet Authentication Service) server.

You should see an additional line for each RRAS server and each IAS server in the Agent Distribution View of the UserLock console. Click Install on the line in order to deploy the agent. After having installed the agent, RRAS or/and IAS services need to be restarted. If both services are installed, you need to stop them both and then only restart them. On Windows Server 2008, you will need to restart the server.

Once the agent is active, RAS sessions are displayed with a different icon (See Quick filter screenshot) in the UserLock console.

You can filter the *User sessions* view to only display RAS sessions (See Quick filter screenshot).



For additional information, please contact IS Decisions at one of the following:

3.1. VPN sessions with a RRAS server

There is one limitation when protecting VPN sessions on Windows RRAS service: the client IP address is not provided, so you cannot apply IP address or range restrictions to these sessions.

As a workaround, you can make the RRAS service work with the IAS service by using the RADIUS protocol (like a hardware router) and install the IAS agent instead of the RRAS agent.

3.2. Radius sessions with IAS server

There is currently no Hardware Compatibility List of hardware VPN routers or Wi-Fi access point correctly working with UserLock 5.

- VPN sessions on a hardware router

Hardware routers need to be configured to contact the IAS server for **RADIUS authentication and RADIUS Accounting**.

There is no standard field in the RADIUS protocol allowing the RADIUS client (VPN server) to send the name of the client computer. So you cannot set computer name restrictions.

The IP address of the VPN client should be available and allowing to set IP range restrictions but some hardware VPN servers may not provide the information. So first check that the IP address is available in the *Session history* report before configuring IP range restrictions for VPN sessions.

- Protecting a Wi-Fi access point with authentication

This is possible if your access point can authenticate users using RADIUS. However, the hardware needs to follow some guidelines.

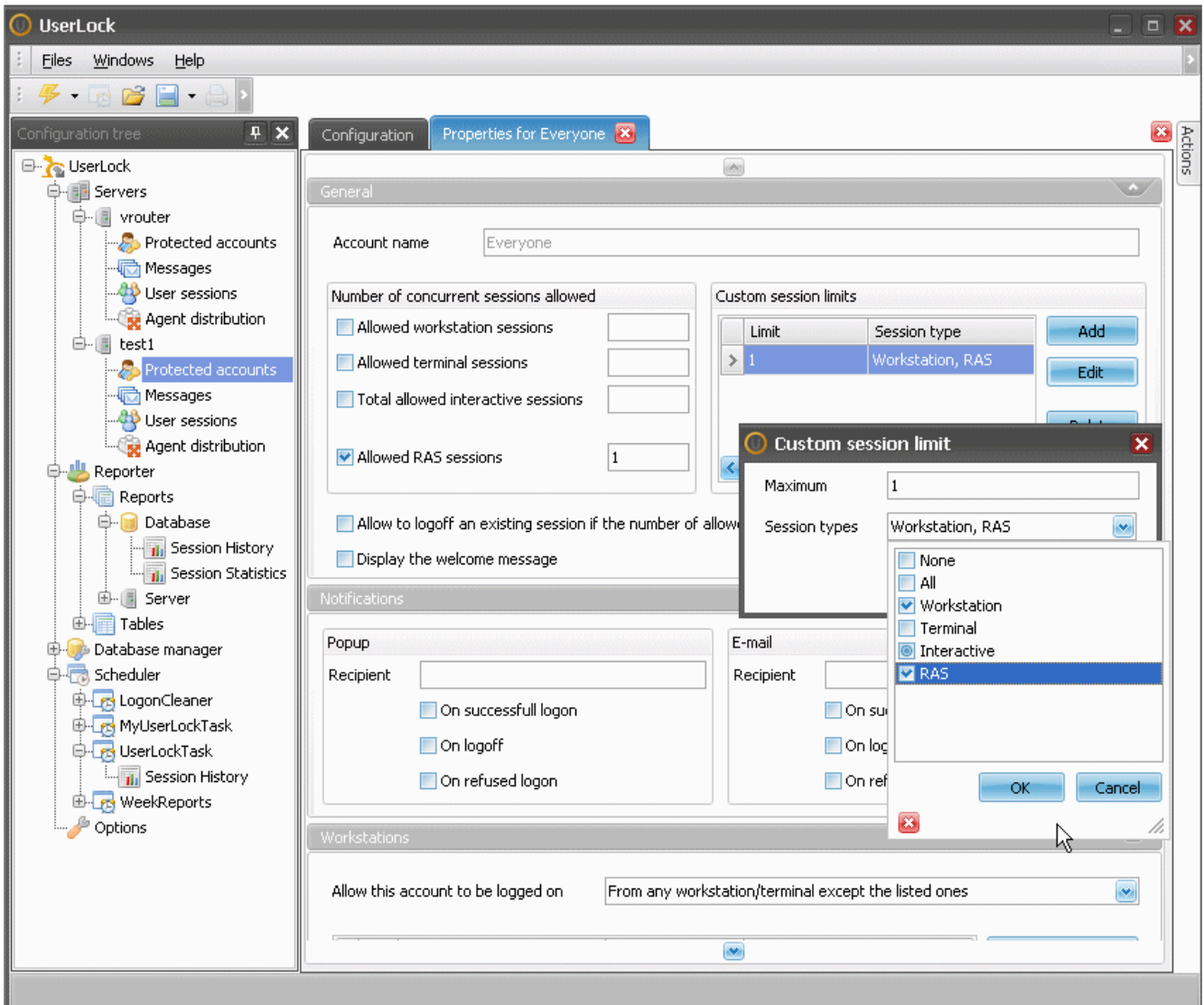
The Wi-Fi access point needs to be configured for **RADIUS authentication and RADIUS Accounting**.

A logoff Accounting event should be sent to the RADIUS server even when a Wi-Fi client unexpectedly disconnects from the access point. Some Wi-Fi RADIUS compliant access points do not follow this rule.

If the Wi-Fi client is a member of the domain, the computer account may be used to authenticate. In this case, UserLock will not handle logons.

For additional information, please contact IS Decisions at one of the following:

3.3. Configuring restrictions for RAS sessions



- Limit concurrent RAS sessions

You can do this in each *Protected accounts Properties* using the new *Allowed RAS sessions* limitation.

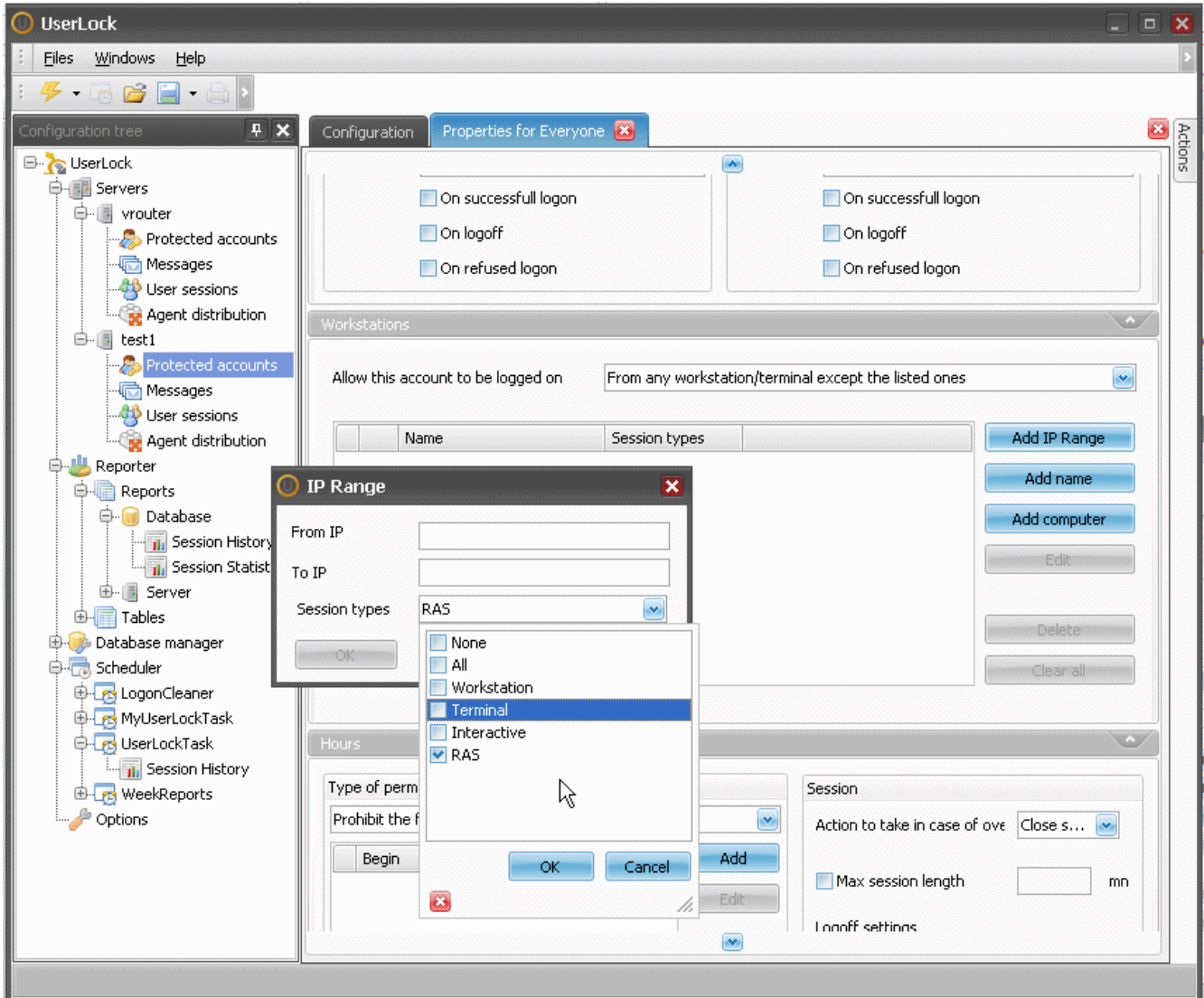
- Custom session limitations

If you want to enforce concurrent session limitations for several kinds of sessions, you can create a *Custom session limit*. For example, if you set a custom limitation of 1 for workstation and RAS sessions, a user will not be able to open a RAS session if he already has an opened workstation session.

For additional information, please contact IS Decisions at one of the following:

- Time restrictions and workstation restrictions

When you configure time restrictions or workstation restrictions, you can now select the kind of sessions that will be impacted by the restriction. So if you want to set a RAS sessions only restriction, unselect all other types of sessions.



For additional information, please contact IS Decisions at one of the following: