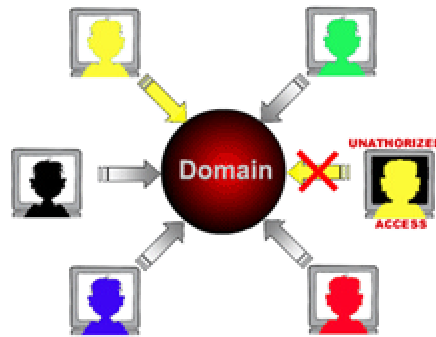


Userlock 2000



Evaluation Guide

12/13/2001

For technical assistance:

support@engagent.com

877-820-7980

engagent®
engage the benefits of domain control

This quick evaluation will require four machines. One will act as the Userlock primary server; the other three will be test workstations. For simplification purposes, all four computers should be on a single sub-network with no routers separating them.

A) Installing UserLock software on server & clients

1. Install the demo¹ on either a workstation or a server—a workstation is fine for a demo despite the warning message that will be displayed.
2. Open the UserLock 2000 console snap-in in the UserLock 2000 program group.
3. In left pane—'Tree', right click UserLock icon.
4. Select your local server (localhost)
5. From the tree, Select 'Agent Distribution' and right click
6. Select 'Properties' and make sure:
 - a. 'Force Reboot' is not checked (this will prevent workstations from being rebooted after the agent has been installed)
 - b. 'Exclude servers from deployment scope' is checked (to prevent the evaluation messages to be displayed on production servers)
 - c. 'Distribution mode' is set to 'deploy the agent'
7. Select (highlight) the three test workstations that will be used during the demo—Please notice that the evaluation version of UserLock will display a copyright/evaluation message each time a user logs on these workstations.
8. Right click on the highlighted workstations and select 'deploy agents' (the agent cannot be deployed to any Userlock server machines). Reboot the workstation(s) to activate the agent.

B) Secure your network

1. Highlight 'Protected Accounts'. Right click and choose either 'new user' or 'new group'. Select the user or group to set restrictions on and click OK. The user or group will be added to the protected accounts list. Generally speaking, Userlock restrictions should be applied to groups instead of users, but for the purposes of the demo, usually it will be best to apply the restriction to an individual user account. You should know the password for that account or have the individual nearby who owns the account.
2. Back in the main Userlock window, double click on the user or group that was added. The user/group properties window will appear. In the 'Number of concurrent logins allowed' section, check 'Define a maximum number of workstations' and type in a '1' in the text box to the right. Click Apply. This means that this account will no longer be able to be logged onto two different Userlock-protected computers at the same time.
3. You can also define the workstations where an account should be authorized to logon to or not. Click on the "Add computer" button in the "Workstations" tab and enter the name of one of the test workstations to prevent this user from logging onto that workstation.

Now the user or group you've configured can only be logged onto one of the two workstations that remains accessible to him. Notice that by right clicking on the Userlock server name and choosing properties, the 'Policy Settings' are shown. Most people will want to set this to 'the less restrictive as possible' so that when two restrictions exist for the same user account, it will allow the higher number of logins to occur.

¹ Ensure you use a domain account with administrator rights for the installation.

C) See UserLock in action

1. Once all of the workstations are rebooted, log onto the test machine that has been specified in the workstations tab using the restricted account. You should not be able to do so because you have configured this account so he can access any workstations except the one you have entered.
2. Then try to log onto one of the two other test machines using the same account. You should now be able to do so as the workstation is not listed in the restrictions list.
3. Try now to logon on the last workstation without logging off the user from the preceding one; UserLock will prevent you to logon as the account has been configured not to allow more than 1 session to be opened at a time.
4. Now logoff from the workstation used during step 2.
5. And try again to logon to the workstation used during step 3. The logon will now be granted.

D) Track your users

1. Once a user has logged in, its status should appear on the 'User sessions report' scope node in the Userlock 2000 console snap-in. It allows you to see in real-time where each of your users are logged on.
2. Now open the UserLock program files directory using the Explorer and open up the file named userlock.log with Notepad. You will see all of the succeeded logon/logoff history. This file is a central repository for all logon and logoff activity. Contrary to Security event logs, it contains only interactive logons and its contents won't be spread across all domain controllers.
3. You may also track users by activating notifications for some events. In the snap-in, double-click again on the account you have configured in the "Protected accounts" scope node. Activate the popup notification on failed logon and enter the name of the UserLock server into the recipient text-box.
4. Now try to logon on a different computer than the one the account is currently logged on to. Once the logon has been rejected, a dialog-box will be displayed on the server detailing what happened.

Appendix

Notice that all userlock messages can be customized by clicking on the 'Messages' scope node then double clicking on the message to be changed (note that the message name may not be fully shown by default... drag the column separator to the right to expose the entire name).

Agents can be distributed automatically to all workstations by selecting 'Agent Distribution' (right click) and then select 'Start'. This will push out the agent to all workstations without having to select all workstations from list. Be sure that Userlock works correctly on some workstations before using automatic agent deployment. We recommend that Automatic agent deployment be done after hours and that 'Force Reboot' is selected in the 'Agent Distribution' scope node properties.