UserLock® vs Microsoft® LimitLogin

This document reviews how Microsoft® LimitLogin and IS Decisions UserLock® achieve logon management, and focuses on the concurrent connections restriction features provided by these 2 software products.

Concurrent connections: a highly underestimated vulnerability

As more and more companies resort to Microsoft server software to manage their networks (**19% sales increase Microsoft Credits Server Sales for Income Gain in Q1 2005** http://www.redmondmag.com/news/article.asp?EditorialsID=6414**),** the ill known yet largely handicapping and critical security flaw still remains omnipresent on a majority of networks, allowing direct access for data leakage, user lockout, workstation downtime…

Microsoft originally tried to address this major issue with an unsupported tool called Cconnect, provided in its *Windows NT/2000 Resource Kit*. However, due to the complexity to implement, the limited and poor functionality, the constraints and the additional flaws(!) the application actually generated, few and far between are those known still actually using it.

With the venue of Active Directory, Microsoft has been back to the drawing board; and whereas one would have thought that they would have properly addressed the issue, they are in fact back with another unsupported tool, responding only partially to requirements and equally awkward to deploy and maintain: LimitLogin.

LimitLogin

Here is the beginning of Bill Boswell's (Microsoft Certified Professional Magazine) very meticulous and precise breakdown on how to deploy LimitLogin:

> "LimitLogin requires a bit of effort to deploy. For one thing, it performs a Schema modification. For another, it creates a new partition in Active Directory. It also requires configuring a Web server with the .NET Framework and ASP.NET and setting it up to do delegated Kerberos authentication. Finally, it requires distributing client packages that support communicating with the Web server via SOAP (a lightweight protocol for exchanging structured information in a distributed environment).
>
> *Whoa.* Don't stop reading. It's complicated, but not impossible. Really."

Source: **Keeping Users at bay** - http://www.mcpmag.com/columns/article.asp?EditorialsID=938

Well, we stopped as, beyond the pure complexity of the installation, the results of this unsupported and free tool are: irreversible changes to the AD Schema, not so free updates for all workstations running anything other than W2K Pro (SP4) or XP (SP1), Windows 2003 Server Edition for the Domain Controller, an IIS server…

UserLock

UserLock® is a third party software utility, developed by IS Decisions providing concurrent connection restriction functionality as well as additional features to optimize and secure user network access. Since 1999, UserLock® has gained a worldwide reputation and is a best-seller within areas where workstations are shared, notably education, health and government.

UserLock® benefits of prestigious clients such as:

▸ l'ONU	▸ University of Alabama	▸ Bergdorf Goodman
▸ La Croix Rouge	▸ Bradley University	▸ Lockheed Martin
▸ Le US Department of Justice	▸ University of Luxembourg	▸ BMW
▸ NY State Organized Crime Task Force	▸ Sterling Bank	▸ Luxottica
▸ Danone	▸ ING Direct	▸ Cegelec
▸ University of Pennsylvania	▸ InterAmerican Development Bank	▸ …

UserLock is user-friendly and will install in minutes on a standard Windows server (NT 4(SP4), 2000/2003 Server).

The configuration wizard will automatically deploy a 100kb dll to selected workstations.

Users and/or groups can be limited in simultaneous sessions as well as from which workstation(s) they can connect.

The administration console displays real-time information and allows complete remote session management with full control and popup / email notification features.

Reporting, besides multiple filtering options, includes workstation usage statistics.

UserLocks latest release, version 3.03, includes features that comply with HIPAA requirements:
(*45 CFR 164.308(a)(5)(ii)(C) Implementation Specification (ADDRESABLE): Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies*).

Comparison

To give a precise and concise view of each solution's capacities:

Feature	UserLock	LimitLogin
Technology	GINA dll	Logon scripts
AD schema modification needed	No	Yes
IIS server needed	No	Yes
Supported client OS	Windows NT4/2000/XP/2003 (no Service Pack requirements)	Windows 2000 SP4, Windows XP SP1, Windows server 2003
Integrated deployer	Yes	No
Software to deploy on clients	Just the UserLock agent needs to be deployed (100 KB dll)	A msi package needs to be deployed
Supported domains	Windows NT4/2000/2003	Windows 2000/2003 (at least one 2003 DC is required)
Define login limit by group	Yes	No (A script needs to be executed to change the limit for all users of a domain or an OU)
Ability to set workstation restrictions	Yes	No
Ability to customize messages displayed to the user	Yes	No
Printable reports	Yes	No (Only CSV or XML)
E-mail & popup notifications	Yes	No
Keep the logon/logoff history in a database	Yes	No
Log lock/unlock events	Yes	No
Is the product supported ?	Yes	No