UserLock®
User logon security for Windows Active Directory
“UserLock works alongside Active Directory to better protect access to Windows systems. With specific and customizable user login rules and real-time monitoring, UserLock reduces the risk of external attacks and internal security breaches while helping to address regulatory compliance.”
User Logon Security for Windows Active Directory

PROTECT, DETECT AND REACT TO ALL USER’S ACCESS TO MICROSOFT WINDOWS SERVER-BASED NETWORKS

UserLock offers stronger security for Windows user logins, without impeding end users or frustrating IT teams. Harden your defence against unauthorized network access and compromised credentials.

ACCESS CONTROL AND PROTECTION
Set and enforce non-intrusive, context-aware access controls that define network access conditions for all Windows users.

DETECTION AND RESPONSE
Real-time monitoring and risk detection tools immediately alert you to suspicious logon activity so you can take action quickly – crucially before that activity becomes a serious problem.

USER SECURITY EDUCATION
Guide and disseminate good end-user security behaviour through alerts and notifications on users own trusted access 'in situ', to help users avoid careless mistakes and discourage malicious actions.

1. GUARD AGAINST UNAUTHORIZED ACCESS USING COMPROMISED CREDENTIALS THAT ARISE FROM EXTERNAL ATTACKS

2. ELIMINATE THE RISKS FROM POOR USER SECURITY BEHAVIOUR (PASSWORD SHARING, UNATTENDED WORKSTATIONS...)

3. VERIFY AUTHENTICATED USERS’ CLAIMED IDENTITY AND ATTRIBUTE ALL ACTIONS TO AN INDIVIDUAL USER TO DISCOURAGE MALICIOUS ACTIVITY

4. REDUCE THE NUMBER OF INCIDENTS OF NON-COMPLIANCE. USERLOCK SUPPORTS MANY REGULATORY REQUIREMENTS OF PCI DSS, HIPAA, ISO27001...
UserLock is a client server application capable of auditing and controlling different types of user access connections.

**NON-DISTURPTIVE TECHNOLOGY**
No modifications are made to Active Directory or its schema. UserLock works alongside Active Directory to extend not replace its security.

**FAST AGENT DEPLOYMENT**
A micro agent is deployed automatically (or manually) on all machines. Once installed all access connections are detected and saved in the UserLock database.

**FAST IMPLEMENTATION**
Hosted on any server member of the domain. Managed remotely on workstations or through a web console anywhere on the network (mobile, tablet)

**ALL SESSION TYPES**
UserLock offers several agent types according to the types of session it has to monitor, workstation, terminal, Wi-Fi & VPN and IIS
How UserLock Works

GENERAL PROCESS DESCRIPTION

The user enters their credentials to log on or to establish a connection to the domain network. These credentials are verified and validated against Active Directory. If the authentication process fails, the connection will be refused by Windows and UserLock does not intervene.

The agent will however notify the UserLock server about this logon failure.

Different agents are available depending on the connection type to be audited and the technology used to configure these connections. The general process is the same regardless of the agent type.
If the authentication is successful, the UserLock agent will transmit to the UserLock server all information about the context of the connection requested. The UserLock server will then process and analyze the data transmitted by the agent to check access control rules, trigger any alerts, refresh session information and save the user connection event in the database. The server then communicates its decision to the agent regarding the acceptance or refusal of the connection requested.
On a connection event of a domain user to the network, the UserLock agent transmits to the server a set of data. This set includes information on:

**Connection event type**
- Logon, reconnection, disconnection, logoff, lock, unlock.

**Connection type requested**
- Workstation, terminal, Wi-Fi, VPN, IIS.

**The user**
- Domain, username.

**The source**
- Machine or device name, IP address.

This information is retrieved by the agent itself when the connection event is submitted by the user, and sent encrypted to the UserLock server, which determines the time of the connection request and saves all in its database. Thus all user connection information performed on agent hosts are collected and stored centrally.
THE EXPLOITATION OF REAL-TIME AUDITED DATA
User Access Control – Permanent and temporary rules

SET AND ENFORCE NETWORK ACCESS CONDITIONS FOR ALL WINDOWS USERS WITHOUT FRUSTRATING OR IMPEDING END USERS

All data audited at the moment of attempted connection is analyzed to verify if the user requesting the connection is subject to access control rules.

Context-aware access control

Transparent to the user, these controls help verify authenticated users’ claimed identity to protect against unauthorized access and compromised credentials.

- Number of simultaneous initial access points
- The type of connection: workstation, terminal, IIS, Wi-Fi and VPN
- The total number of concurrent connections and by type of connection
- The origin of the connection
- The time of the connection
- The connection time quota and by requested type of connection

Defined for a user account, a user group and/or an organizational unit of users, the rules allow or deny a connection requested by a domain user account. UserLock then transmits this decision to the agent of the relevant system.
Initial Access Points

UserLock can analyze what the sequence is of a user’s connections to determine whether a session is a new point of entry to the network or a connection performed from an existing session.

A new point of entry is considered as the initial access point for the user initiating the connection.
Initial Access Points

RESTRICTIONS TO VERIFY AN AUTHENTICATED USERS’ IDENTITY

Limiting the number of initial access points to one will ensure that the user won’t be able to open a session from a second location.

If you don’t limit the number of concurrent sessions allowed, the user will be able to open as many sessions as they want, but only if they are children/nested sessions of the same initial access point.

The results are displayed in real time in UserLock with icons that tag sessions to differentiate an initial access point from a nested session.
Concurrent Sessions

The limit of concurrent sessions allowed can be used in association with the limit of initial access points to define how many and which types of session (workstation, terminal, Wi-Fi/VPN and IIS) a user can open from the same initial access point.

In the example where workstations are limited to 1, if a user tries to open a second session while the previous is open, their logon will be denied.

If the number of initial access points allowed is not configured, the number of permitted concurrent sessions will still be effective.
Control Access by Origin

Define and manage the workstations/terminals, IP range and session type from which a user, group or organizational unit may log on. For example, to restrict a user to connect only from a specific machine.

Within UserLock you can query Active Directory to check and select named workstations, users, groups or organizational units.
Control Access by Time

MANAGE AND RESTRICT CONNECTION HOURS

The 'Hour restrictions' section allows you to define, by session type, periods of time during which users can or cannot logon to the network. For example, to prevent access connections outside certain hours.

When the authorized time frame has expired, a warning notification can be displayed to users before automatically initiating a forced session logoff or session lock.

You can also choose to apply the time restrictions according to the machine's local time zone.
Control by Time Quota

MANAGE AND RESTRICT CONNECTION HOURS

A connection time quota can be assigned to determine the maximum period of time connected to the network during a recurring period (day, week, month...) for specified session types.

The ‘consumed time’ per user can be displayed and managed from the UserLock console.
UserLock can automatically log off sessions after a specific idle time. Every session of the user account is closed after a chosen idle time period. It can be defined by user, group and Organizational Unit.
Additional Options

A ‘SINGLE ACTIVE SESSION’ OFFERS FLEXIBILITY FOR THE USER

By distinguishing between an active session and a locked session, UserLock can:

• Allow users to log off an existing session remotely if the number of allowed sessions has already been reached.

• Allow only one unlocked interactive session at a time. Any other session will be automatically locked or disconnected by UserLock.
Connection Alerts for IT Administrators

IMMEDIATE RESPONSE TO ALERT ON OR AUTOMATICALLY BLOCK SUSPICIOUS LOGON EVENTS

Real-Time Alert Notifications

The user rules also include alert notifications for defined connection events. Two types of alerts can be defined: pop-up messages and email messages.

The data audited during the connection, whatever the decision taken (authorized, refused or failed), are analyzed and compared against the criteria of alert triggers — defined for the user requesting the connection.

These alerts are triggered to inform the predefined recipients for the following connection events: logon, logoff, lock, unlock, disconnect, reconnect, logon denied by Windows and logon denied by UserLock.

For example alerts can be set for failed logon attempts, attempts to log on to default accounts, logon activity during non-working hours...
Connection Alerts for End Users

ALERTS TO POTENTIAL COMPROMISED OR STOLEN CREDENTIALS

Warnings (real-time) direct to the user

An option allows a pop-up message to be displayed for every session of a user when their credentials are used from another machine or used to open another connection.

The audited data collected at connection attempts also allows the user to be alerted every time their credentials are used on the network.

This alert message indicates the source of the connection, the type of the connection, the time and their status (accepted or denied).

The user is then invited to report this event to their IT team if they are not responsible for the requested connection, and to change their password if potentially compromised.

A UserLock administrator can customize this alert message and choose which connection events will trigger it.
A Risk Indicator on User Access for IT Administrators

BETTER IDENTIFY SUSPICIOUS OR INAPPROPRIATE ACCESS BEHAVIOR

Risk status & real-time alerts

By correlating each user’s access events with their customized access controls, each user’s ‘risk status’ evolves according to the user’s actions when accessing or attempting to access the network.

Six statuses are available to highlight activity that could help detect anomalies in user connection.

Activity deemed as risk or high risk are clearly flagged in the console. Alerts can also be sent to administrators on a changing risk status.

Threshold triggers on what is considered as risk can also be adapted to suit an organizations own needs.

The ‘risk status’ is information and does not result in blocking or denying a user connection — the goal is to highlight risk situation to allow administrators to respond appropriately.
High-Risk Status

A USER IS CONSIDERED TO HAVE A POTENTIALLY HIGH-RISK BEHAVIOR WHEN:

1. The number of sessions open is over the limit defined for their account.
2. Frequency of failed logons by UserLock or/and Windows is over the frequency tolerated.
3. The number of initial access points open is over the limit defined for their account.
4. Two simultaneous initial access points are detected from inside and outside the local network.
**High-Risk Status**

**FREQUENCY OF FAILED LOGONS**

The repetition of connection failures over a period of time may be a sign of identity theft attempts or connections attempts from disapproved resources for the user.

UserLock agents inform the server about every denied logon from Windows and the associated reason (invalid password, account locked, account disabled, Active Directory policies, etc.) UserLock also saves all denied logon due to UserLock policies and the detailed reason (simultaneous limit, unauthorized machines, forbidden time ranges, etc.).

This information is not only saved in the database but also stored in memory within the UserLock service to allow an iterative analysis.

It is therefore possible to set a threshold of tolerance for logons denied by Windows or by UserLock beyond which the user status will be switched to high-risk.

<table>
<thead>
<tr>
<th>After</th>
<th>5 logons denied by UserLock in less than 30 minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>After</td>
<td>2 logons denied by Windows in less than 30 minutes</td>
</tr>
</tbody>
</table>

1. **THE NUMBER OF SESSIONS OPEN IS OVER THE LIMIT DEFINED FOR THEIR ACCOUNT**
2. **FREQUENCY OF FAILED LOGONS BY USERLOCK OR/AND WINDOWS IS OVER THE FREQUENCIT TOLERATED**
3. **THE NUMBER OF INITIAL ACCESS POINTS OPEN IS OVER THE LIMIT DEFINED FOR THEIR ACCOUNT**
4. **TWO SIMULTANEOUS INITIAL ACCESS POINTS ARE DETECTED FROM INSIDE AND OUTSIDE THE LOCAL NETWORK**
High-Risk Status

DETECT SIMULTANEOUS INITIAL ACCESS POINTS FROM INSIDE AND OUTSIDE THE LOCAL NETWORK

1. The number of sessions open is over the limit defined for their account.
2. Frequency of failed logons by UserLock or/and Windows is over the frequency tolerated.
3. The number of initial access points open is over the limit defined for their account.
4. Two simultaneous initial access points are detected from inside and outside the local network.

Example of a user opening a workstation session in the local network while a VPN connection is open from outside.
A user is considered to have a potentially risky behavior when:

1. Connection attempt blocked due to the Active Directory account status.
2. Users opening a new session from an existing session with different credentials.
3. The number of sessions open by session type is over the adjustable thresholds.
4. The number of initial access points open is over the adjustable threshold.
Risk Status

A USER OPENING A NEW SESSION FROM AN EXISTING SESSION WITH DIFFERENT CREDENTIALS

Example of a user opening a terminal session from a workstation session with valid but different credentials.

1. CONNECTION ATTEMPT BLOCKED DUE TO THE ACTIVE DIRECTORY ACCOUNT STATUS BEING LOCKED OR DISABLED

2. USERS OPENING A NEW SESSION FROM AN EXISTING SESSION WITH DIFFERENT CREDENTIALS

3. THE NUMBER OF SESSIONS OPEN BY SESSION TYPE IS OVER THE ADJUSTABLE THRESHOLDS

4. THE NUMBER OF INITIAL ACCESS POINTS OPEN IS OVER THE ADJUSTABLE THRESHOLD

UserLock can analyze users' new connections to detect if this is a new point of entry in the network or a connection performed from an existing session, and in this last case, it can compare the credential used. If the credential used to open a child/nested session is different, UserLock is able to switch the user status to the risk level.
Administrators can use the status ‘Risk’ to highlight users with a number of connections that they deem as abnormal. The goal is to detect easily within the console users having a large number of connections and send an alert if necessary — but without blocking users’ access requests. These threshold values are configurable for one or several types of audited connections.

- Connection attempt blocked due to the Active Directory account status
- Users opening a new session from an existing session with different credentials
- The number of sessions open by session type is over the adjustable thresholds
- The number of initial access points open is over the adjustable threshold
## Other Indicative Status

INFORM ADMINISTRATORS OF OTHER USER CONNECTION ACTIVITY

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unprotected</strong></td>
<td>A user is considered as not protected when his account is not member of a Protected account rules and he is not currently eligible to another status.</td>
</tr>
<tr>
<td><strong>Protected</strong></td>
<td>A user is considered as protected when his account is member of a Protected account rules and he is not currently eligible to another status.</td>
</tr>
<tr>
<td><strong>New</strong></td>
<td>A new user is a user opening a session on the network for the first time. UserLock consider a user as new when his account doesn’t have a session history on the network zone monitored or after a period of time in day during which no session activities have been detected. This period of time defined by default to 15 days and can be customized. A user will have this status on his first connection event occurring after [15 ± 3] days.</td>
</tr>
<tr>
<td><strong>Inactive</strong></td>
<td>A user without any open session, known by UserLock and referenced into UserLock logs will be considered as inactive after a time period in day of inactivity on the network. This period of time in day is defined by default to 15 days and can be customized. A user will have this status after a period of [15 ± 3] days of inactivity on the network.</td>
</tr>
</tbody>
</table>
Reporting and Auditing on all Logon and Logoff Activity

Centralizing & Archiving all Events
All user connection information transmitted by the agent are audited and saved centrally in a database. Information stored can be used to generate predefined reports directly from the console.

- **Session history**: The detailed list of every connection (logon, lock, unlock, disconnection, logoff, users, machines, domains, etc.) available for all session types.
- **User status history**: The list of status changes for every user and the reasons.
- **Session statistics**: The total number of sessions, the total time and average time per session for a user on a defined period.
- **Session count evolution**: Changes in the number of all the interactive sessions open on the network.
- **Two additional reports for Wi-Fi/VPN sessions**: History and statistics with additional relevant filters.
- **The ability to view raw data**: Tabled from the database.
- **A tool view allowing you to submit an SQL query**: From the console itself.
REACT IN REAL TIME TO A SPECIFIC SITUATION
Interact Remotely — with all sessions, open or locked

AN IMMEDIATE RESPONSE CAN HELP REDUCE THE RISK OF SECURITY BREACHES

Remote response

React from the UserLock console from any device (smartphone, tablet or computer). Simply selecting on one or several sessions in the UserLock console allows you to launch the following actions on the following session types:

- ‘Workstation’ sessions: Logoff the session, lock the session, send a pop-up message, run a computer command.
- ‘Terminal’ sessions: Logoff the session, lock the session, send a pop-up message, run a computer command.
- ‘IIS’ sessions: Logoff the session, run a computer command.
Immediately Block a User

For any specific user you can block all logon attempts and close all existing sessions remotely, to react quickly to compromised or suspected compromised credentials. Just select the user from the 'User sessions' view and launch the command. Until the user is unblocked, all connection attempts will be denied.
Computer commands

UserLock offers the possibility to launch from the console a predefined computer command or to create your own to run specific jobs or scripts.

Actions can include: remote desktop, remote connection to the computer management console, script, event viewer remote connection, etc.
Adjust user access control rules

SECURITY IS AN ITERATIVE PROCESS

Access security is not a one-time activity. Restrictions should be evaluated and revised periodically so that improvements can be implemented.

User access control rules can be modified at any time for a user or a group, or to create a temporary rule to define an exception for a particular user. All changes are applied in real time and are effective immediately.
DOWNLOAD
A FREE FULLY FUNCTIONAL TRIAL
NOW
WWW.USERLOCK.COM