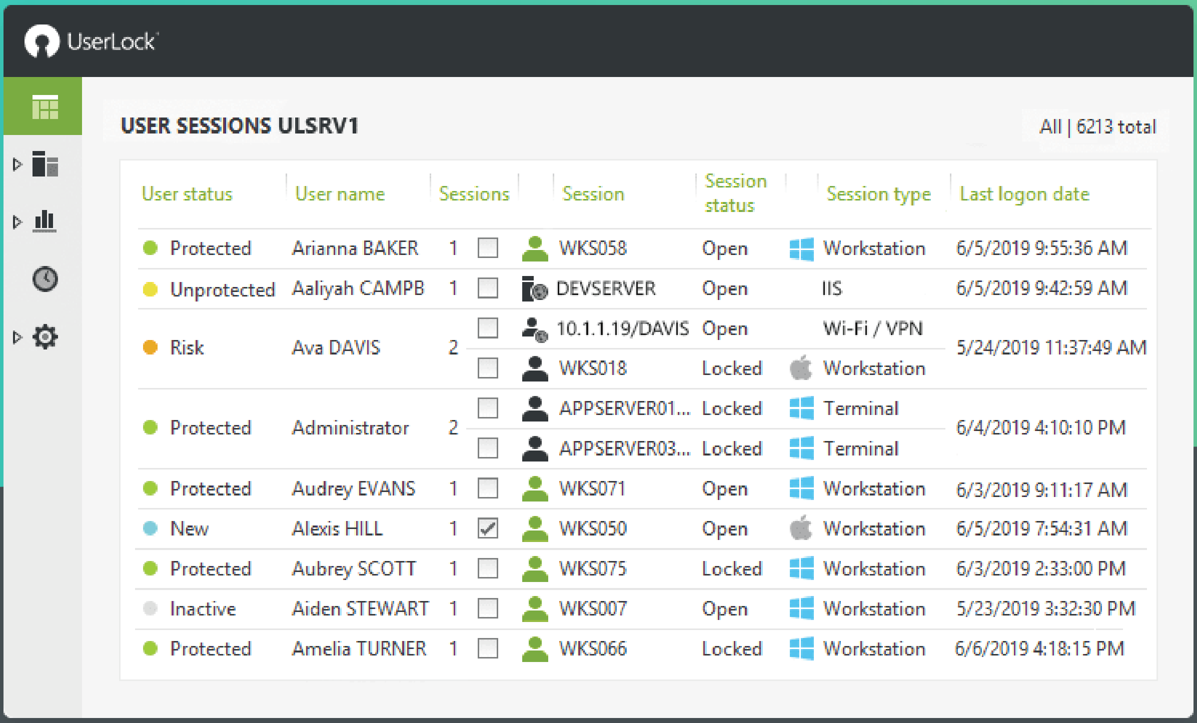
DATASHEET

UserLock®

Multi-Factor Authentication and Access Management. **The Easy Way.**



UserLock

USER SESSIONS ULSRV1

All | 6213 total

User status	User name	Sessions		Session	Session status	Session type	Last logon date
● Protected	Arianna BAKER	1	□	WKS058	Open	Workstation	6/5/2019 9:55:36 AM
● Unprotected	Aaliyah CAMPB	1	□	DEVSERVER	Open	IIS	6/5/2019 9:42:59 AM
● Risk	Ava DAVIS	2	□	10.1.1.19/DAVIS	Open	Wi-Fi / VPN	5/24/2019 11:37:49 AM
			□	WKS018	Locked	Workstation	
● Protected	Administrator	2	□	APPSERVER01...	Locked	Terminal	6/4/2019 4:10:10 PM
			□	APPSERVER03...	Locked	Terminal	
● Protected	Audrey EVANS	1	□	WKS071	Open	Workstation	6/3/2019 9:11:17 AM
● New	Alexis HILL	1	☑	WKS050	Open	Workstation	6/5/2019 7:54:31 AM
● Protected	Aubrey SCOTT	1	□	WKS075	Locked	Workstation	6/3/2019 2:33:00 PM
● Inactive	Aiden STEWART	1	□	WKS007	Open	Workstation	5/23/2019 3:32:30 PM
● Protected	Amelia TURNER	1	□	WKS066	Locked	Workstation	6/6/2019 4:18:15 PM

The **Challenge**

Whether because of exploited users, careless errors, malicious actions or external attacks, your **employees' login credentials can be effortlessly compromised**. And when they are, your anti-virus, anti-intrusion, firewall and other security technologies won't flag anything unusual. Those tools believe that if the person accessing your network enters the right credentials, then they are exactly who they say they are – an authenticated user with authorized access!

Knowing that the majority of data breaches stem from compromised credentials, organizations need to **better protect access for all employee logins** – not just the privileged users/ administrators. Any account with access to data that is sensitive, privileged or otherwise valuable is at risk.

A Comprehensive **Solution**

By adding two-factor authentication (2FA), single sign-on (SSO), contextual restrictions and real-time insight around logon activity, UserLock helps administrators **secure, monitor and respond to user access**, preventing damage before it's done.

And with UserLock, access to any data or resource is now always **identifiable and attributed** to one individual user. This accountability discourages an insider from acting maliciously, and makes all users more careful with their actions. It's also necessary for many organizations to fulfill common compliance or cyber-insurance requirements.

Protection Across Common Use Cases

Learn more

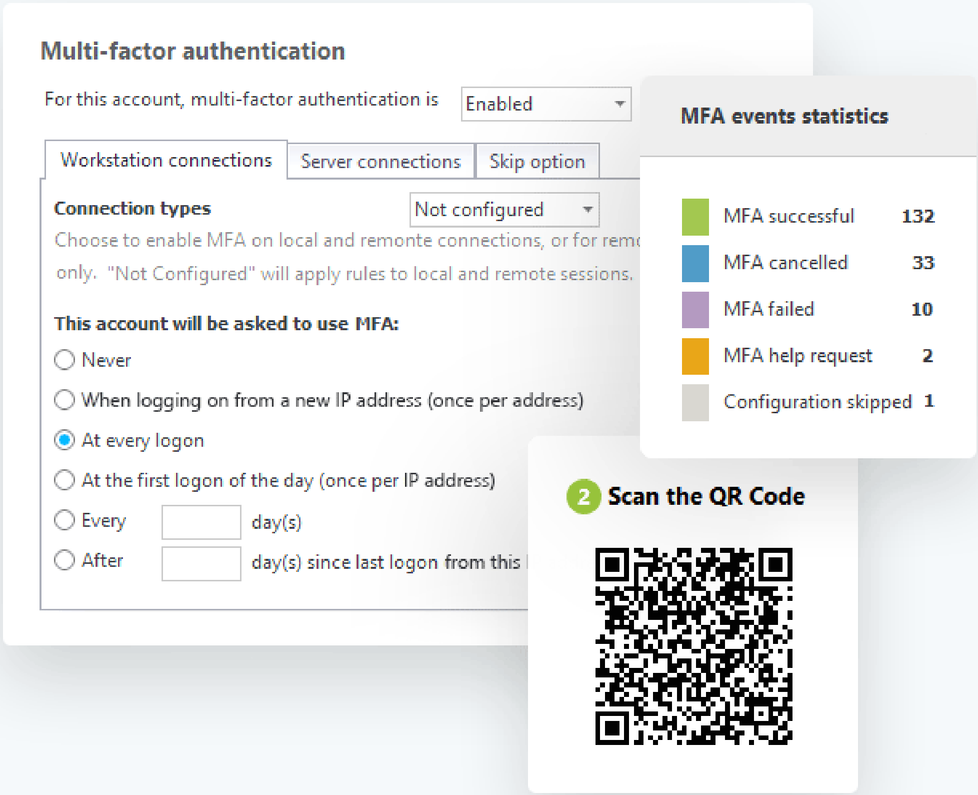
- **Secure** all employee access
- **Secure** privileged access
- **Secure** access to cloud apps
- **Secure** remote access
- **Streamline** session management
- **Get accurate** logon logoff forensics
- **Manage** working hours
- **Meet** compliance & insurance requirements
- **Stop** security breaches

ACCESS SECURITY **FAR BEYOND** NATIVE WINDOWS FEATURES

1

Two Factor Authentication

Verify the identity of all users with strong two-factor authentication (2FA) on Windows logon, Remote Desktop (RDP & RD Gateway), IIS, VPN and Cloud Applications. Using authenticator applications or programmable hardware tokens such as YubiKey or Token 2, administrators can customize the circumstances under which 2FA is asked.



Multi-factor authentication

For this account, multi-factor authentication is: Enabled

Connection types: Not configured

Choose to enable MFA on local and remonte connections, or for remo
only. "Not Configured" will apply rules to local and remote sessions.

This account will be asked to use MFA:

○ Never
○ When logging on from a new IP address (once per address)
● At every logon
○ At the first logon of the day (once per IP address)
○ Every ______ day(s)
○ After ______ day(s) since last logon from this

MFA events statistics

🟩	MFA successful	132
🟦	MFA cancelled	33
🟪	MFA failed	10
🟧	MFA help request	2
⬜	Configuration skipped	1

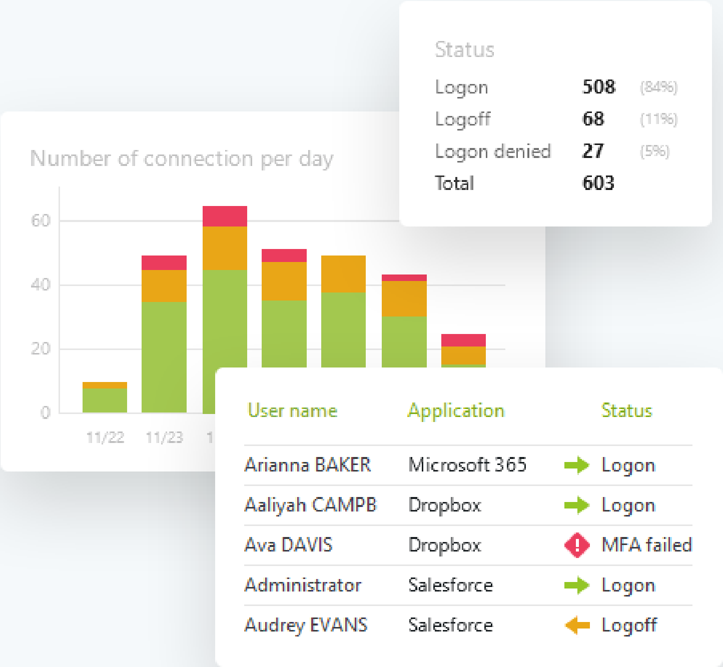
2 **Scan the QR Code**

2

Single Sign-On

UserLock Single Sign-On (SSO) gives employees secure and frictionless access to Microsoft 365 and cloud applications – from wherever they work – using only their on-premises Active Directory (AD) credentials with SAML 2.0 federated authentication.

Organizations can retain AD as the authoritative identity provider, while extending it to work with the cloud.



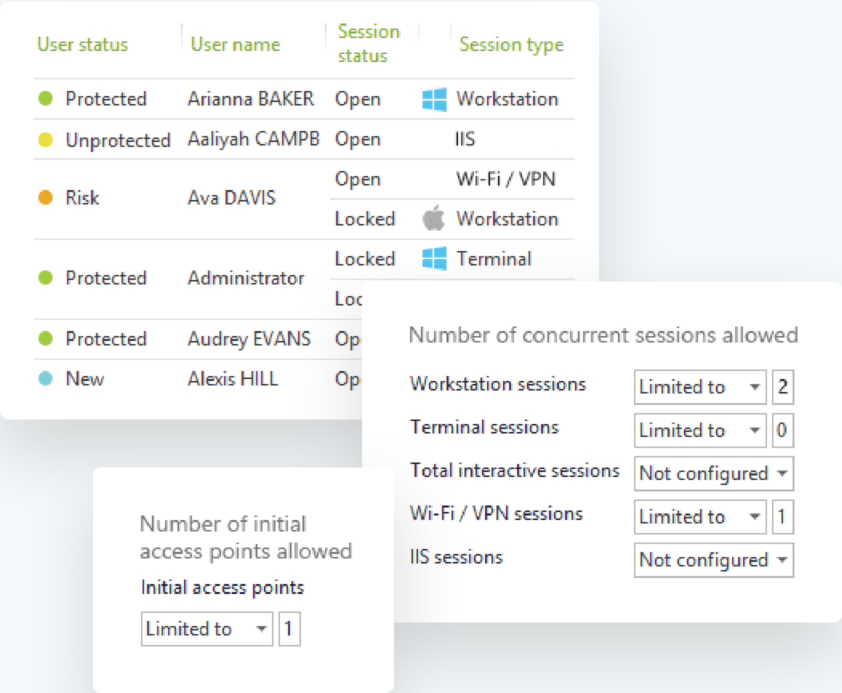
Status		
Logon	508	(84%)
Logoff	68	(11%)
Logon denied	27	(5%)
Total	603	

User name	Application	Status
Arianna BAKER	Microsoft 365	Logon
Aaliyah CAMPB	Dropbox	Logon
Ava DAVIS	Dropbox	MFA failed
Administrator	Salesforce	Logon
Audrey EVANS	Salesforce	Logoff

3

Contextual Access Policy and Restrictions

Administrators can set rules to authorize, deny or limit any login (including remote access) based on contextual factors like machine, location, time, session type, or number of simultaneous connections.



User status	User name	Session status	Session type
● Protected	Arianna BAKER	Open	Workstation
● Unprotected	Aaliyah CAMPB	Open	IIS
● Risk	Ava DAVIS	Open	Wi-Fi / VPN
		Locked	Workstation
● Protected	Administrator	Locked	Terminal
		Loc	
● Protected	Audrey EVANS	Op	
● New	Alexis HILL	Op	

Number of concurrent sessions allowed

Workstation sessions	Limited to	2
Terminal sessions	Limited to	0
Total interactive sessions	Not configured	
Wi-Fi / VPN sessions	Limited to	1
IIS sessions	Not configured	

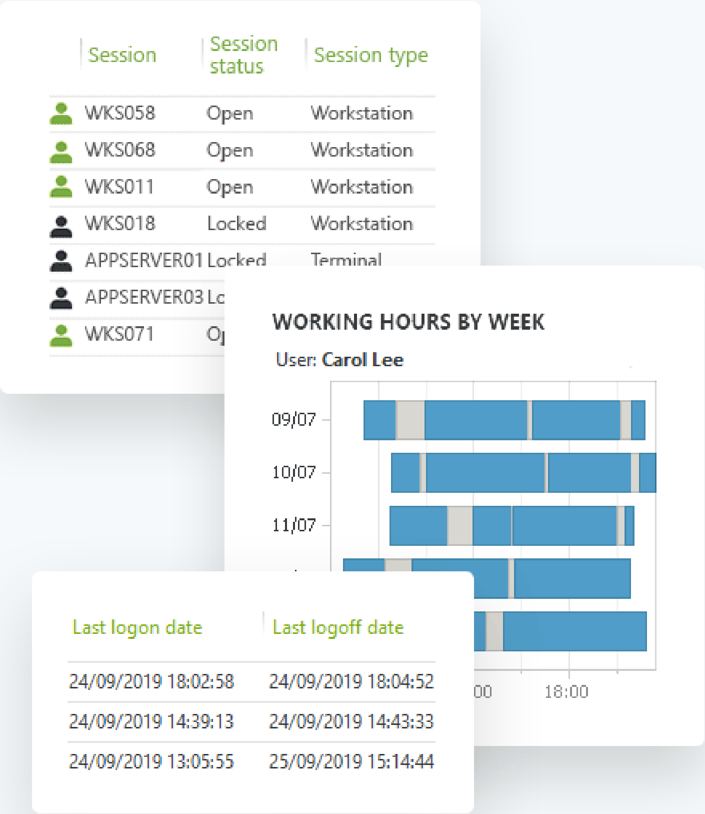
Number of initial access points allowed

Initial access points	Limited to	1

4

Real Time Monitoring and Reporting

Real-time visibility into all user access gives administrators insights into potential threats and the ability to respond to any session, directly from the console. And, a centralized audit for reporting on all AD user login activity allows administrators to report on who was connected, from which system(s), since what time, for how long, etc.

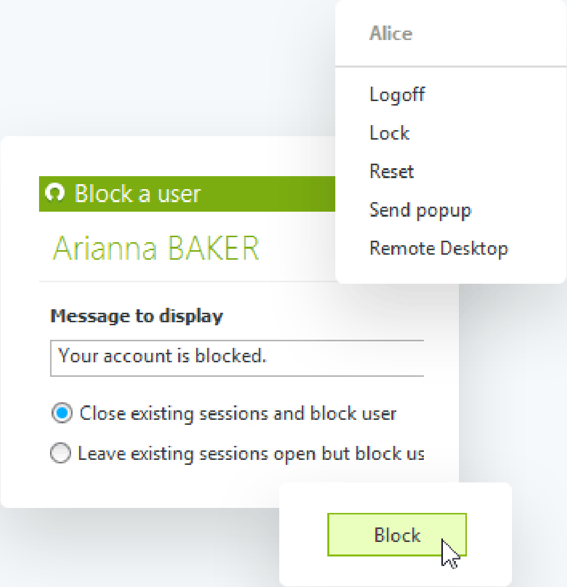


Session	Session status	Session type
WKS058	Open	Workstation
WKS068	Open	Workstation
WKS011	Open	Workstation
WKS018	Locked	Workstation
APPSERVER01	Locked	Terminal
APPSERVER03	Lo	
WKS071	Op	

WORKING HOURS BY WEEK

User: **Carol Lee**

Last logon date	Last logoff date
24/09/2019 18:02:58	24/09/2019 18:04:52
24/09/2019 14:39:13	24/09/2019 14:43:33
24/09/2019 13:05:55	25/09/2019 15:14:44



Block a user

Arianna BAKER

Message to display

Your account is blocked.

● Close existing sessions and block user

○ Leave existing sessions open but block us

5

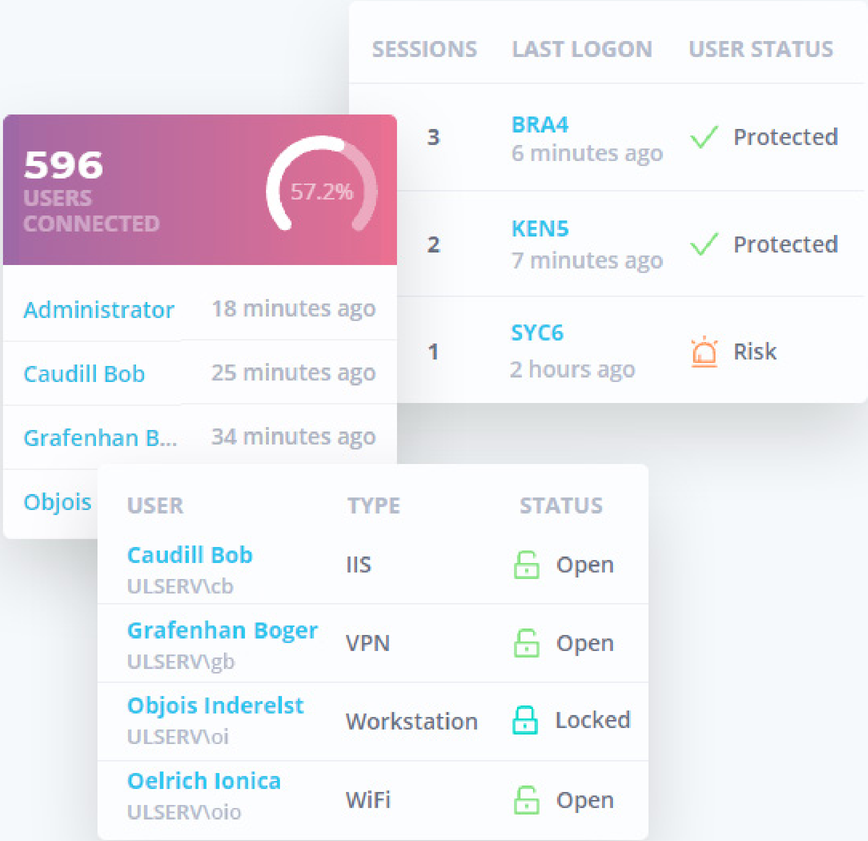
An Immediate Response to Logon Behavior

Allows IT to interact remotely with a suspect session, to lock the session, log off the user, or even block them from further logons.

6

Enhanced Monitoring Response, and Reporting

Download the **new, intuitive UserLock Web App** in version 11.2 to monitor, respond, and report on network sessions quickly and easily, from anywhere.



596 USERS CONNECTED

57.2%

Administrator	18 minutes ago
Caudill Bob	25 minutes ago
Grafenhan B...	34 minutes ago
Objois	

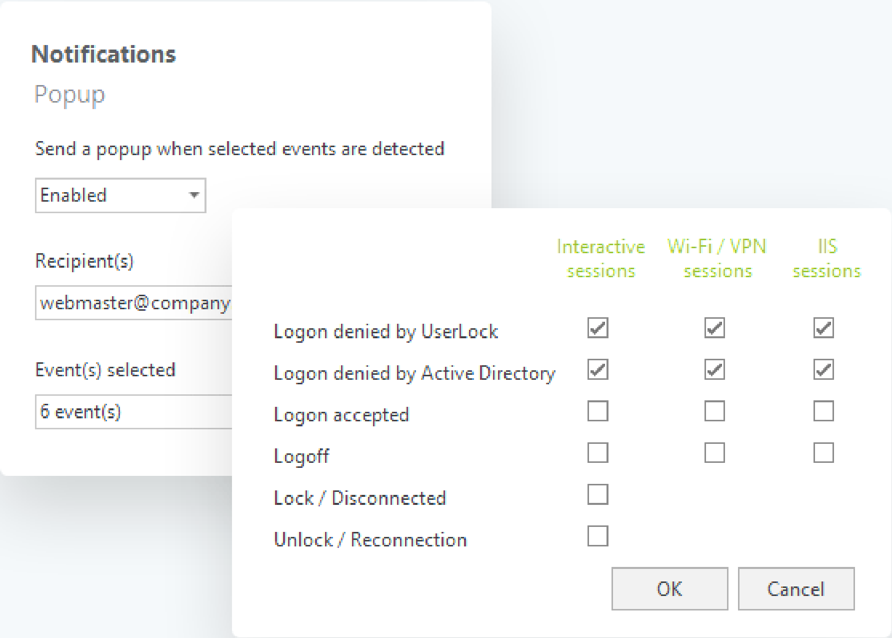
SESSIONS	LAST LOGON	USER STATUS
3	BRA4 6 minutes ago	✓ Protected
2	KEN5 7 minutes ago	✓ Protected
1	SYC6 2 hours ago	Risk

USER	TYPE	STATUS
Caudill Bob ULSERV\cb	IIS	Open
Grafenhan Boger ULSERV\gb	VPN	Open
Objois Inderelst ULSERV\oi	Workstation	Locked
Oelrich Ionica ULSERV\oio	WiFi	Open

7

IT and End-User Alerts

Set up alerts to notify IT and the user themselves of inappropriate logon activity and failed attempts.



Notifications

Popup

Send a popup when selected events are detected

Enabled

Recipient(s)

webmaster@company

Event(s) selected

6 event(s)

	Interactive sessions	Wi-Fi / VPN sessions	IIS sessions
Logon denied by UserLock	☑	☑	☑
Logon denied by Active Directory	☑	☑	☑
Logon accepted	□	□	□
Logoff	□	□	□
Lock / Disconnected	□		
Unlock / Reconnection	□		

THE **GO-TO ACCESS MANAGEMENT PARTNER** FOR ON-PREMISES AND HYBRID ACTIVE DIRECTORY ENVIRONMENTS!

Reduce Complexity

Works seamlessly alongside your existing investment in Active Directory, reducing complexity and frustration for IT teams. No modifications are made to accounts, structure or schema.

Easily Adopted

Easily adopted by end-users with the best balance of security and usability. Granular controls allow for customized restrictions that protect access without getting in the way of employee productivity.

Easy Set-Up

Quick to deploy and intuitive to manage, administrators can set up UserLock in minutes on a standard Windows Server.

Scale Effortlessly

AD Group level controls and an automated deployment engine make implementation easy for any number of users.

Enables Cost-Effective Security

Building on your investment in AD, UserLock offers additional, effective and affordable security.

Supports Powershell Integration

Helps expedite and/or schedule certain tasks and execute personalized requests on the information within UserLock.

Supports Webhooks & API

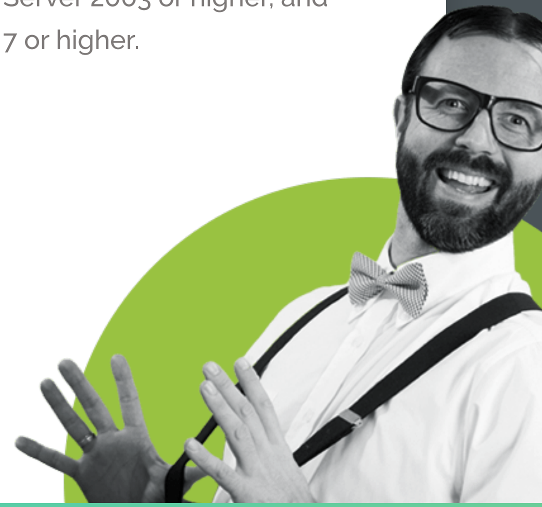
Integrate the valuable data managed by UserLock with other solutions to improve overall IT security management.

Includes Failover Safeguards

A UserLock backup server can be installed to guarantee failover.

System Requirements

Supported operating systems include Windows Server 2003 or higher, and Windows 7 or higher.



TRY THE FULL VERSION FOR FREE WITH OUR 30 DAYS TRIAL

START A FREE TRIAL

SYSTEM **REQUIREMENTS**

Domain	**Active Directory required (for workgroups, see the Standalone Terminal Server UserLock server type).** *Functional level of forest and domain: Windows Server 2003 or higher.*
Operating systems	UserLock supports the following operating systems: › **For UserLock Server**: Windows Server 2003 and above › **For UserLock Console**: Windows 7 and above, Windows Server 2003 and above › **For workstations to protect:** Windows XP and above, Mac El capitan and above › **For servers to protect:** Windows 2003 and above, Citrix, any terminals using RDP sessions or ICA sessions.

› FOR ALL INFORMATION ON REQUIREMENTS

ABOUT **IS DECISIONS**

IS Decisions is a global software company specializing in access management and MFA for on-premises and hybrid active directory environments. Trusted by over 3400 organizations, we offer proven solutions for both small to medium-sized businesses (SMBs) and large organizations, including some of the most regulated and security-conscious organizations in the world.

IS Decisions
Technopôle IZARBEL - Créaticité Bât. A - BP12 - 64210 Bidart - FRANCE
Phone: +33 5.59.41.42.20 - Fax: +33 5.59.41.42.21
www.isdecisions.com - info@isdecisions.com

Silver
Microsoft
Partner