



UserLock[®]

360° MFA and access management

- Secure on-premise Active Directory identities
- Close security gaps across all access types
- Gain real-time threat visibility
- Extend secure access to the cloud



What's your end game?

Put security where it's most likely to prevent a breach

Access is the common factor in almost every cyber attack.

No access, no breach.

What types of access to protect?

All access.

Across all users.

In all circumstances.

Start with what you have

On-premise Active Directory is a critical resource – not an afterthought.

Cloud-first access security can be counterproductive:

- Requires managing another directory
- Increases attack surface
- Opens security gaps with cloud identity providers

What you need in an access security solution

- Secure all types of access
- Increase visibility to spot threats quickly
- Integrate with existing systems
- Meet compliance and cyber insurance requirements
- Simplify your job, not complicate it

Most access security solutions

- 1 Frustrate users
- 2 Add complexity
- 3 Create inefficiencies
- 4 Have hidden costs

How UserLock is different

- 1 Access-focused zero-trust security
- 2 Seamless AD integration
- 3 Total, 360° security coverage
- 4 Flexible policy customization

A unique advantage: Drawing on 24 years of proven expertise

With over two decades of continuous improvement, we have deep expertise in securing access to Active Directory.

An established reputation built over two decades

Trusted by 3400+ clients
across diverse sectors.

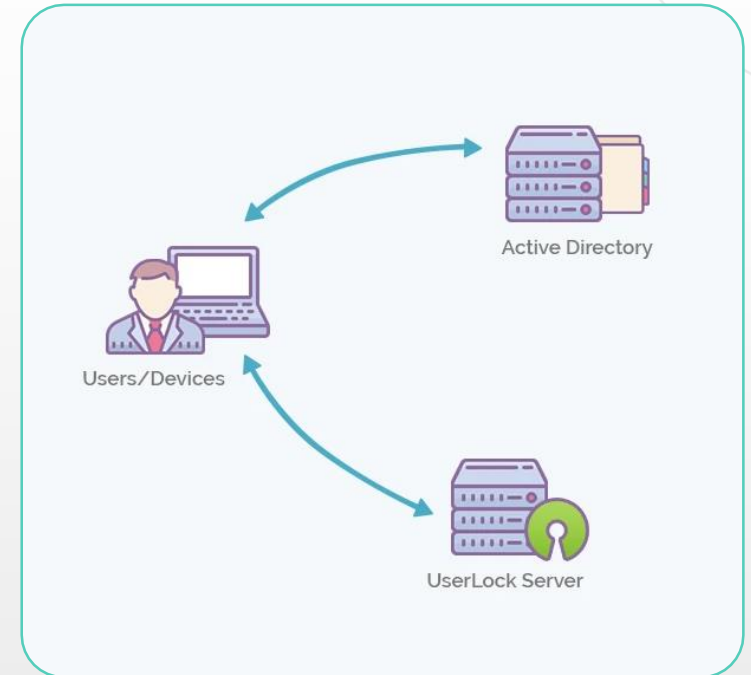


UserLock and zero-trust security

- Implement "never trust, always verify"
- 360° visibility on network access
- 360° MFA and access controls

UserLock's integration with on-premise Active Directory

- Effective security for a modern on-premise environment
- Constant synchronization with Active Directory
- Seamless transition for your team
- Support for hybrid infrastructure



UserLock closes common access security gaps

Userlock ensures policy enforcement across all scenarios:

- Offline logins
- Off-LAN logins
- VPN-less connections
- Remote connections
- Outside connections

UserLock's flexible policy enforcement

- Balance security and productivity
- Enforce role-based and contextual access restrictions
- Tailor MFA policies to your team
- Choose how often to prompt for MFA

This account will be asked to use MFA

Not configured ▼

Not configured

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)

After a given time

After a given time since the last logon from this IP address

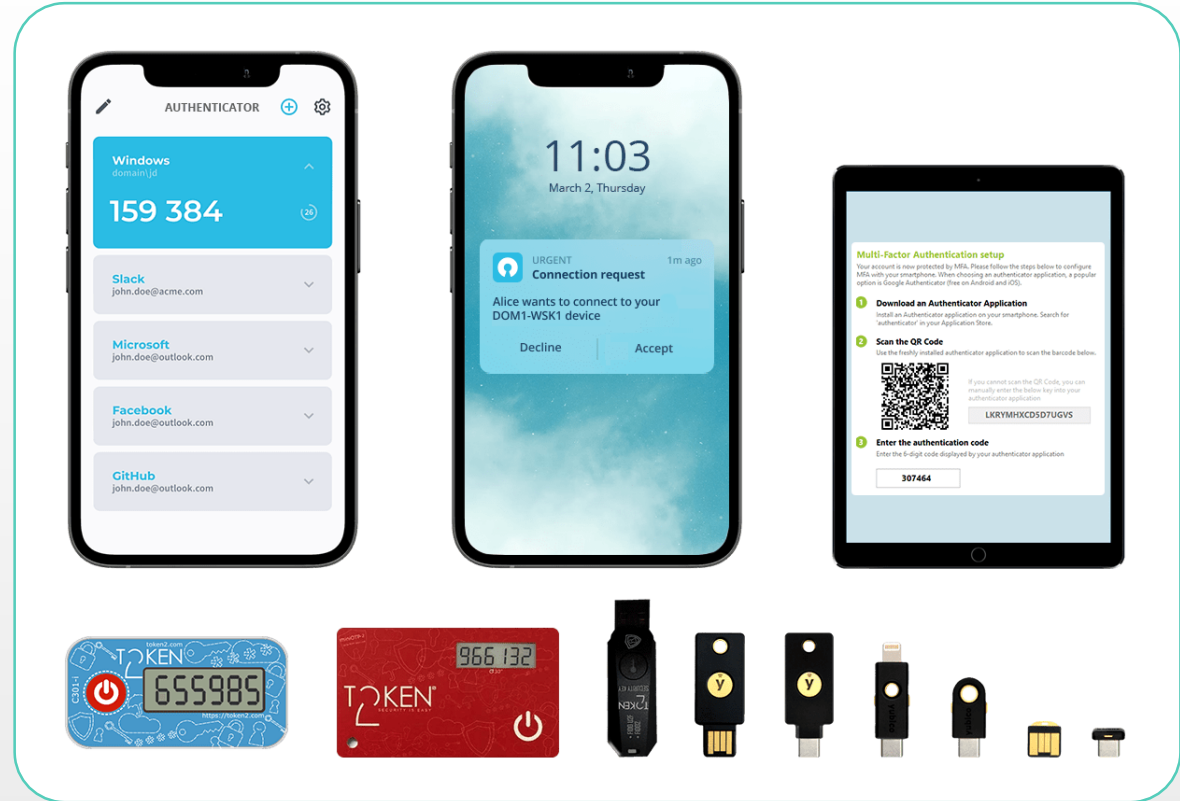
Not configured ▼

Not configured ▼

Multi-factor authentication

Verify and protect the identity of all users with strong two-factor authentication on Windows logon, Remote Desktop (RDP, RD Gateway, RemoteApp), IIS, VPN, and Cloud Apps.

UserLock supports authenticator applications, Push notifications via the UserLock Push app, and programmable hardware tokens such as YubiKey or Token 2.



Customized MFA

Avoid prompting your users for MFA more than needed. With UserLock define the frequency and circumstances for MFA.

Multi-factor authentication

For this account, multi-factor authentication is **Enabled**

Connections **Skip option**

Edit mode: All session types at once

Session type	Connection types	This account will be asked to use MFA
All	Remote	Not configured
Workstation	Remote	Not configured
Server	Remote	Never
IIS	Remote	When logging on from a new IP address (once per address)
VPN	Remote	At every logon
SaaS	Remote	At the first logon of the day (once per IP address)

After a given time

After a given time since the last logon from this IP address

MFA for remote working

Enforce MFA to secure a variety of remote connection types (RDP, VPN, IIS).

When no such secure connection exists, MFA is still enforced via an internet connection.

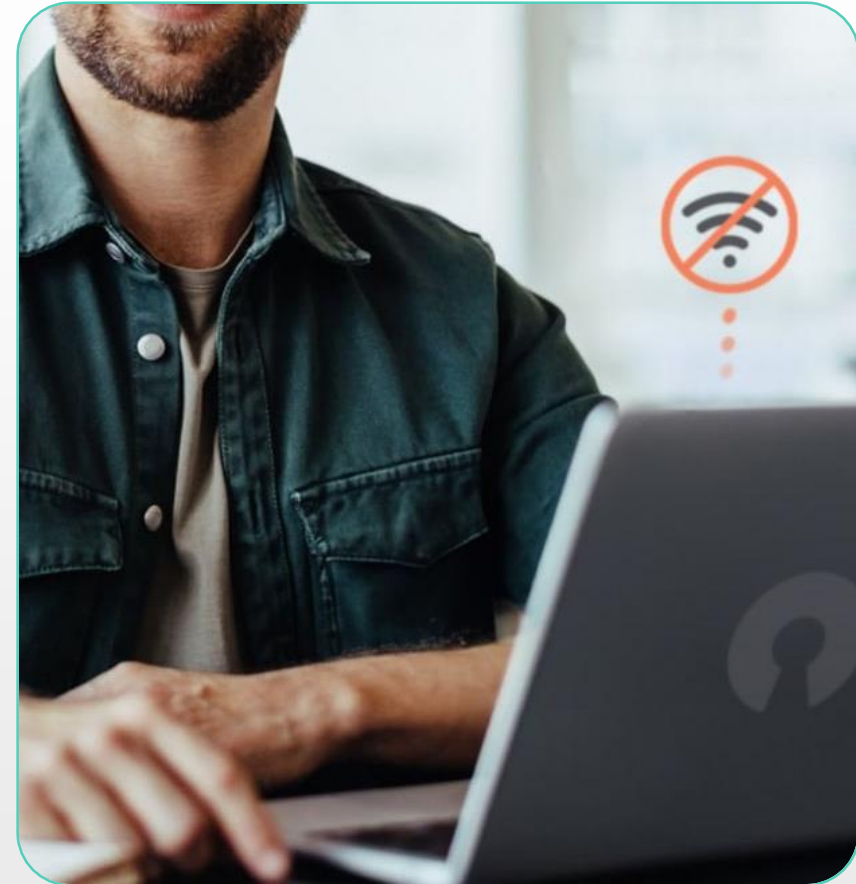
The screenshot displays the UserLock configuration interface for Multi-Factor Authentication (MFA). It features three overlapping panels:

- Connection types**: A dropdown menu with options: "Not configured", "All", "Remote", "From outside" (highlighted in green), and "Not configured".
- This account will be asked to use MFA:** A section with radio button options:
 - ☐ 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)
- Multi-factor authentication**: A section with the text "For this account, MFA is" followed by a dropdown menu set to "Enabled".

Offline MFA

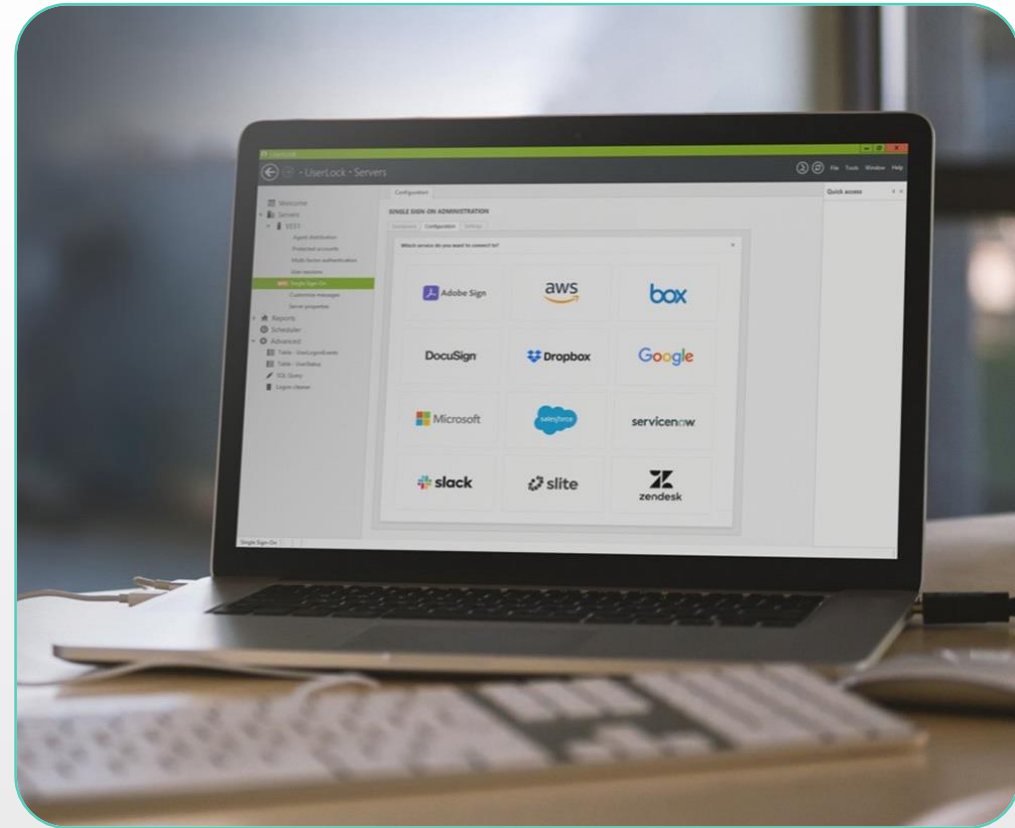
With secure on-premise hosting, UserLock MFA needs no internet connection on-site.

An agent can also protect a remote machine with MFA when there's no internet connection.



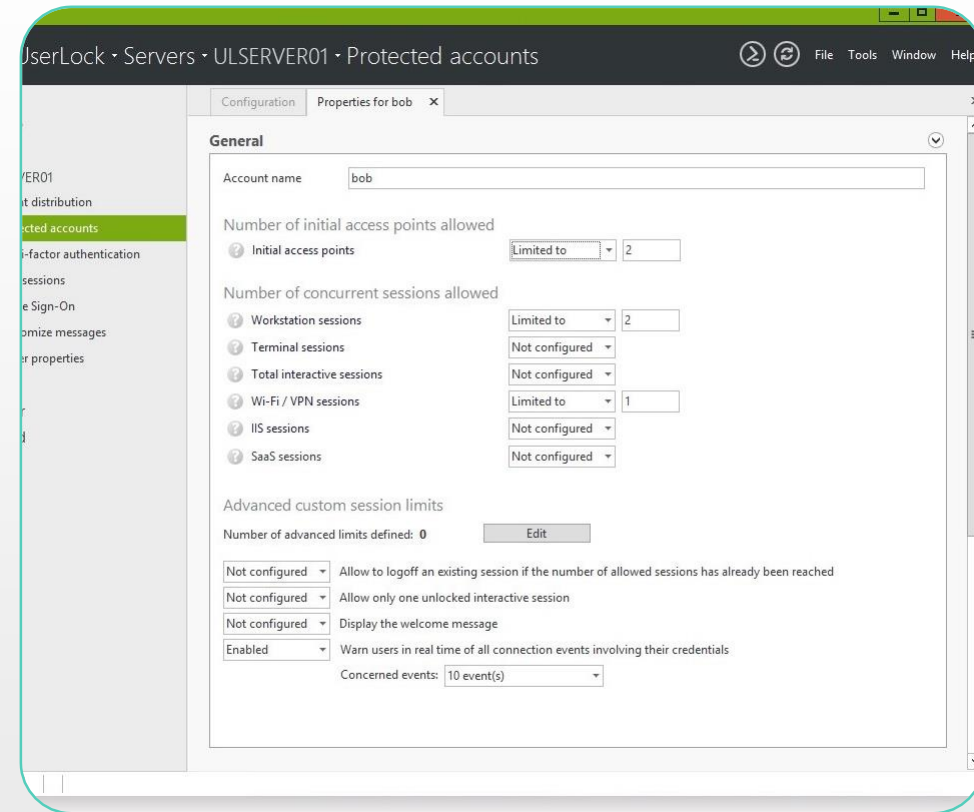
Single sign-on

UserLock provides SAML federated authentication to Microsoft 365 and cloud applications using on-premise Active Directory (AD) identities.



Contextual access controls






Reduce the risk of inappropriate access. Limit who can logon when, from where, for how long, and how frequently, and restrict specific combinations of logon types.



Session management

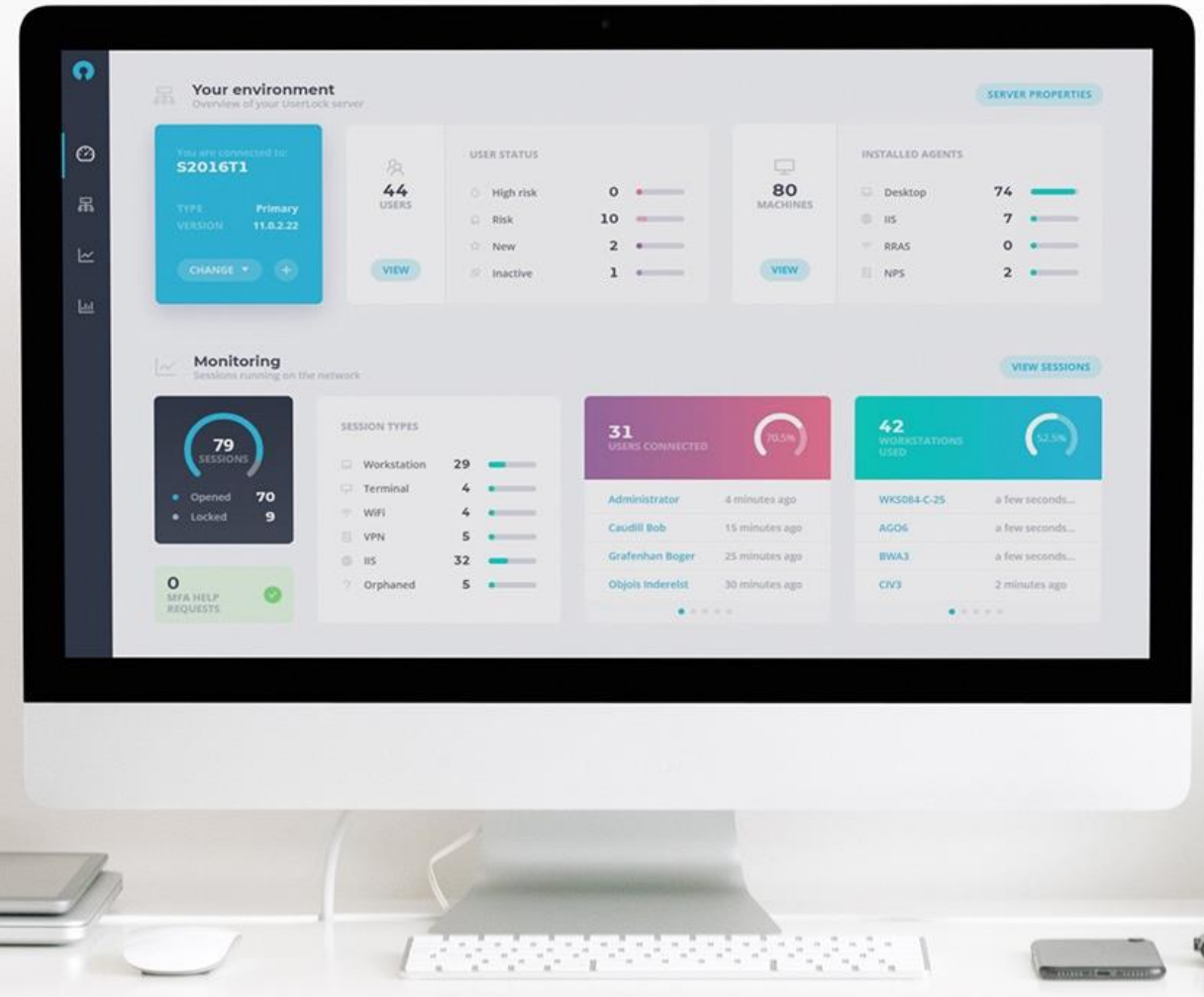
Real-time visibility serves as the basis for enforcing policy, alerting and interacting on any access events.

A centralized audit provides detailed reports to support forensics and prove regulatory compliance

USER	TYPE	STATUS	MACHINE (CLIENT → REMOTE)		LOGON DATE
Bob CAUDILL SERV\cb	IIS	 Open	CAUDILLB 10.1.1.103	→ ULSERV2	a few seconds ago
Boger GRAFNHANB SERV\gb	Terminal	 Locked	GRAFNHANB 10.1.1.102	→ ULSERV2	2 minutes ago
Indereist OBJOISI SERV\oi	VPN	 Open	OBJOISI 10.1.1.122	→ 10.1.1.21	6 minutes ago
Clark MATTC SERV\mc	Workstation	 Open	MATTC 10.1.1.22		7 minutes ago
Klamber SERV\jk	IIS	 Open	10.1.1.107	→ ULSERV2	7 minutes ago

The UserLock web application

Monitor and respond to network sessions quickly, easily, and from anywhere. Simplify daily management and widen UserLock access for all IT.



Real-time visibility on user access

See who is accessing your network, how, and when, without scrolling through Windows event logs and bouncing between different platforms to get a complete picture.

All users (1042) ▾					
NAME	USER STATUS	SESSIONS	LAST LOGON		
Aganb Alica DOMAIN\aalica	✓ Protected	1	PRT1 5 hours ago	Actions ▾	
Aganoff Alice DOMAIN\aalice	✓ Protected	2	QAT1 a day ago	Actions ▾	
Amileta Billel DOMAIN\abillet	⚠ Risk	1	SMR1 an hour ago		
Audrey Evans DOMAIN\aeavans	✓ Protected	2	RWA1 an hour ago		
Brayden Coy DOMAIN\bcoy	✓ Protected	3	SRB1 2 hours ago		

All machines (526) ▾				
NAME	IP ADDRESS	AGENTS	LAST CHECK	
Caudill Bob Workstation	10.1.2.72	DESKTOP ▾	a min. ago	
Grafenhan Boger Server, IIS	10.1.1.22	DESKTOP ▾ IIS ▾	a min. ago	
Objois Inderelst Server, IIS	10.1.1.18	DESKTOP ▾ IIS ▾	a min. ago	
Oelrich Ionica Workstation	10.1.2.74	DESKTOP ▾	a min. ago	
Amerschuber Workstation	10.1.2.45	DESKTOP ▾	a min. ago	

Detect and stop threats

- Set up alerts and respond instantly to threats with remote computer commands via the UserLock console
- Spot risky behavior quickly with the risk indicator
- Log off users with suspicious activity in one click



Use cases

How UserLock helps Active Directory environments of all sizes and sectors meet compliance and security goals.

Combining SSO with MFA to protect all access

SYMTA Pièces was looking to enable single sign-on (SSO) and multi-factor authentication (MFA) for Office 365 using on-premises Active Directory (AD) credentials.

UserLock SSO now streamlines login to various Office 365 apps, and reduces the burden on employees of entering complex passwords multiple times a day.

The IT team can choose how often to prompt for MFA at a granular level – setting a lower frequency for on-site access, but asking for MFA at each connection for remote access.



MFA with YubiKey for Quebec police



The City of Trois-Rivières is required to use MFA in order to comply with government regulations.

UserLock matched the need of supporting YubiKey on both on-site and RDP connections. It also offered easy user enrollment, a centralized console and detailed reports on all access and access attempts.

Thanks to UserLock, the Police Directorate were able to comply with regulations and simplify the day-to-day work of the IT team.



MSP chooses UserLock for insurance-approved, on premise MFA



A Minnesota-based MSP that served small and large enterprises needed an Insurance-approved MFA solution.

The solution needed to work without an internet connection, handle all access attempts to the network, support both YubiKey and mobile phone authentication, and be customizable for different user access policies.

Hosted on-premises and linked directly to Active Directory, UserLock was found to be easy to implement, lightweight for users, and secured access without impeding employee productivity.



Active Directory MFA for US city following a ransomware attack



The City of Keizer needed to strengthen their access security after being hit by a ransomware attack.

To comply, the Department had implemented Duo 2FA, but they didn't find it to be very easy to set up or user friendly. So, they sought a new solution that they could easily deploy across all user and administrative accounts, from all departments.

According to the City, UserLock is an IT managers' dream: the deployment and implementation were flawless, zero complaints from end-users, easy-to-use, affordable and it integrates simply with Active Directory.



Meeting the Central Bank of Kuwait's compliance policy

Following an audit by the CBK, an emerging bank was found not to have a solution in place to restrict active directory concurrent sessions.

With UserLock, IT administrators can set and enforce access rules that restrict from where, when and how long an authenticated Active Directory user may logon.

The complete UserLock set up was done in a single day and the team was able to easily integrate it into the bank's system. With compliance now achieved for concurrent sessions, the bank is looking at implementing MFA and other contextual access restrictions to secure employee's access.



Managing access for hundreds of users at a leading real estate company



The IT Team at Orange Coast Title Company needed to be able to remotely manage users' sessions and comply with many regulations around multi factor authentication.

UserLock's real-time visibility and reporting into all users' sessions gave administrators the overview they were looking for, and the ability to quickly review and respond to any incident or event.

UserLock's MFA proved to be a game-changer for the IT team as it represents one of the functionalities most demanded by many regulations.



Offline MFA for remote working

Dobbs Peterbilt needed to be sure that their senior employees who worked remotely and travelled extensively were secured as much as possible.

IT required MFA at login on all remote connections, even when offline. UserLock MFA requires no internet connection and can prompt users for a second authentication factor when connecting via RDP or VPN.

With MFA in place wherever remote users are working, access is secured and auditors are satisfied.



DOBBS PETERBILT



Easy to install MFA for a large enterprise

With over 2000 employees working remotely, MFA protection was needed, with or without a secure network connection.

UserLock proved easy for the IT Team to install and configure across multiple sites to protect on-site and remote access. Opting to use Google Authentication App , users found the self-enrollment process quick and simple.

With MFA in place wherever remote users are working, access is secured, even for offline access.



Our clients

Trusted by over 3400 organizations, UserLock scales easily across organizations of any size, including some of the world's most regulated and security-conscious.



We wanted to add multi-factor authentication for RDP and local on-site connections. The installation only took a few minutes and the initial setup was very easy. The low cost of the solution, the ease of implementation, the quality of the documentation and the 30 day free trial convinced me.

Mathieu Vandal

System Administrator, City of Trois-Rivières, Quebec



We wanted a multi-factor authentication solution to secure access to jump servers and meet local audit requirements. The technology had to be provided by a system that was hosted locally (on-premise) and worked with corporate AD credentials. We found UserLock very easy to implement and will recommend to other branches within the bank.

IT Officer

Multinational Banking Group, Hong Kong



UserLock is a great software that has simplified our working day. Employees work in large, open-space offices, where no user has their own machine. UserLock allows us to verify that the user who authenticates is who they say they are. We also found the reports to be an extremely useful tool. The visibility on all user connection events provides us a central audit across the whole network. With this they could easily view the start and end of a session opened on the network to spot any anomalies or suspicious behavior.

José Miguel Villafuerte

IT Infrastructure Manager, Teleperformance, Mexico



All in all, the UserLock solution allows you to do what it says it will do—control all aspects of user login activity. The beauty of the solution is that you can do this in a granular way, and it is highly customizable. The auditing and reporting are very detailed and provide great visibility into activities around user login activity.

Brandon Lee
4sysops.com



Relatively simple to deploy via UserLock, the implementation of MFA on an infrastructure significantly enhances security, especially with the current trend and the boom in remote working.

Florian Burnel
it-connect.fr



It was very easy to add two factor authentication for our in-house AD users with UserLock. This was a huge compliance requirement in our organization. The real-time insight regarding user logons gives administrators the best way to know if any unauthorized login is happening. Also with the help of limiting number of sessions for the elevated users, this tool helps to manage secure elevated access.

5 Star Review on Gartner Peer Insights

Senior System Administrator, United States



UserLock was love at first sight!

It is the perfect combination – easy to use software, with good support. I've never seen MFA implement so easily before.

Cameron Rezvani

Senior Systems Engineer, Orange Coast Title, United States



In this digital age, computer access is essential for students and teachers alike, but this access needs to be managed properly as it can lead to significant misuse. UserLock is the ideal solution that helps us meet our network access objectives effectively.

Don Manning

Server Administrator, Albany City School District, United States



*Great product and best price/value on the market.
The product was very easy to setup and use for our
organization. The features included were exactly
what we were looking for to meet compliance
regulations and improve risk management.*

5 Star Review on Gartner Peer Insights

Senior IT Project Manager in Professional Services, United States

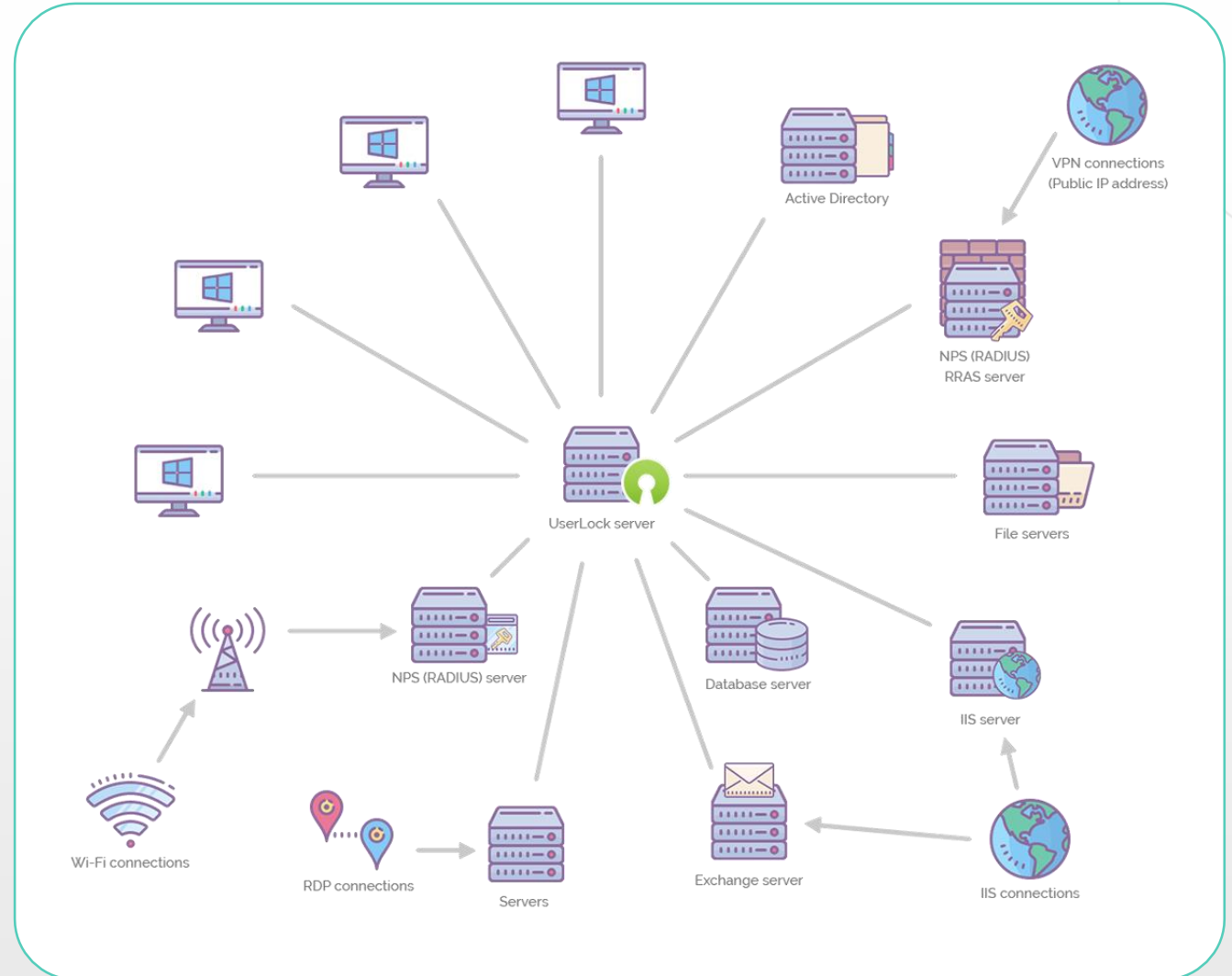
“

*The perfect access security partner for
Windows Active Directory environments.*



Infrastructure

UserLock is a **client server** application capable of **auditing** and **controlling** different types of user access connections.

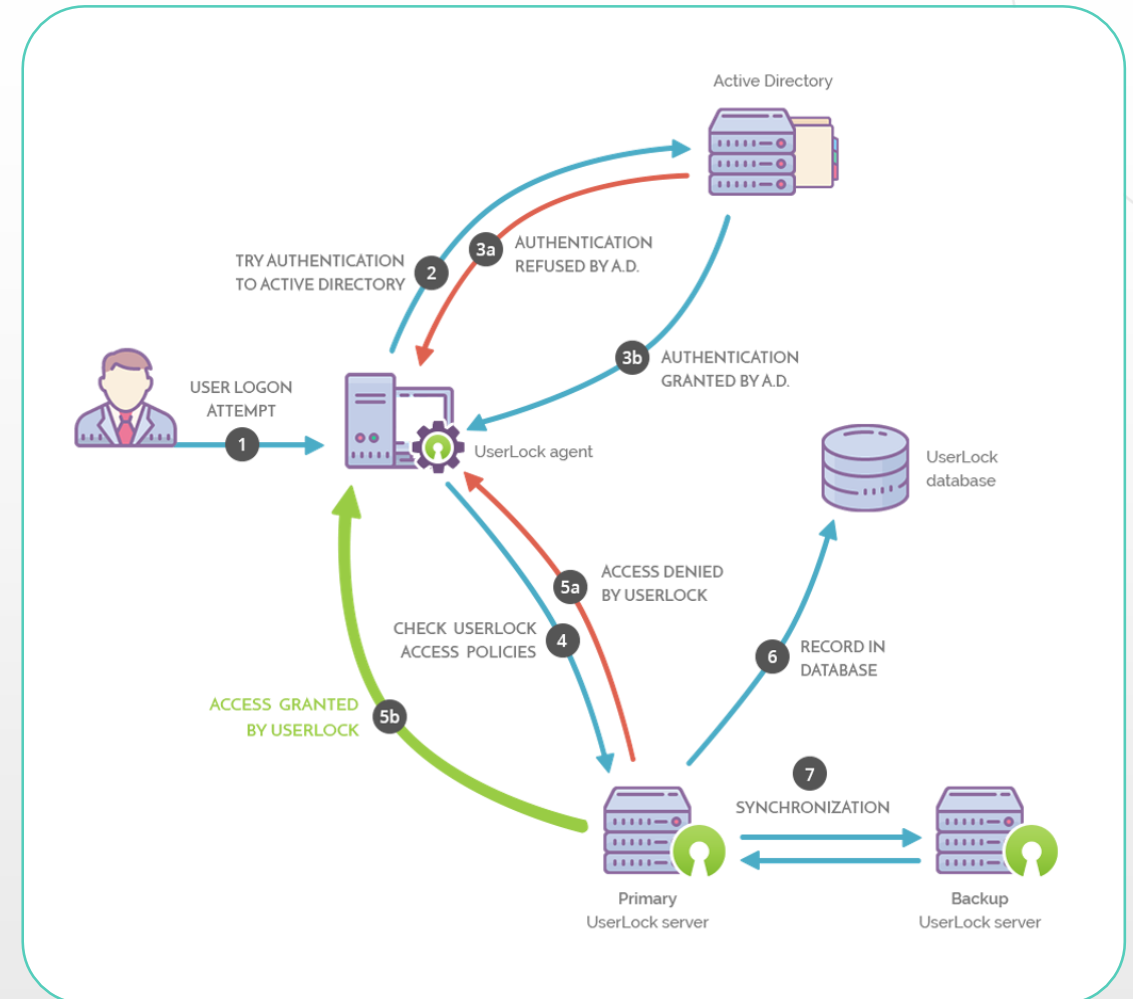


How UserLock works

General process description (1/2)

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.



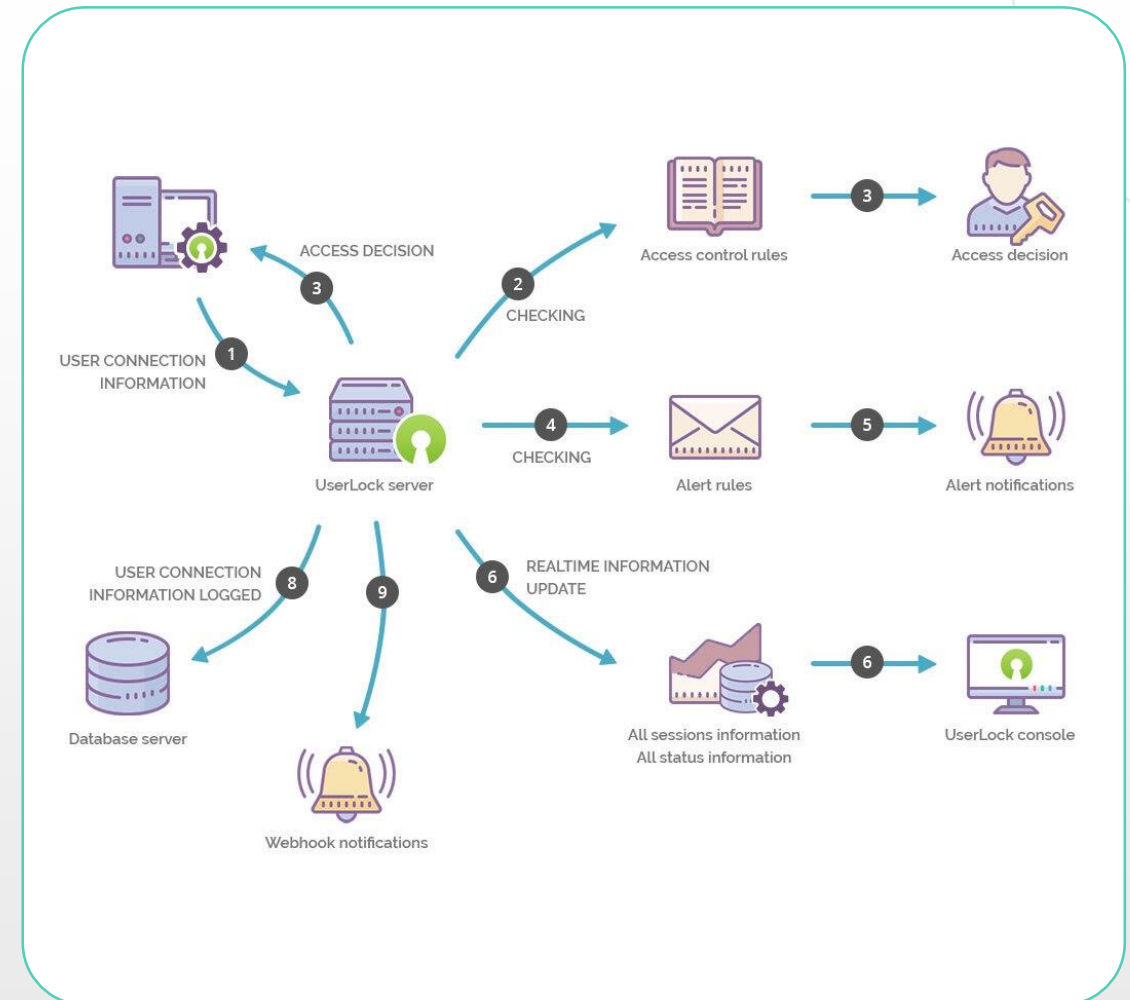
How UserLock works

General process description (2/2)

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.

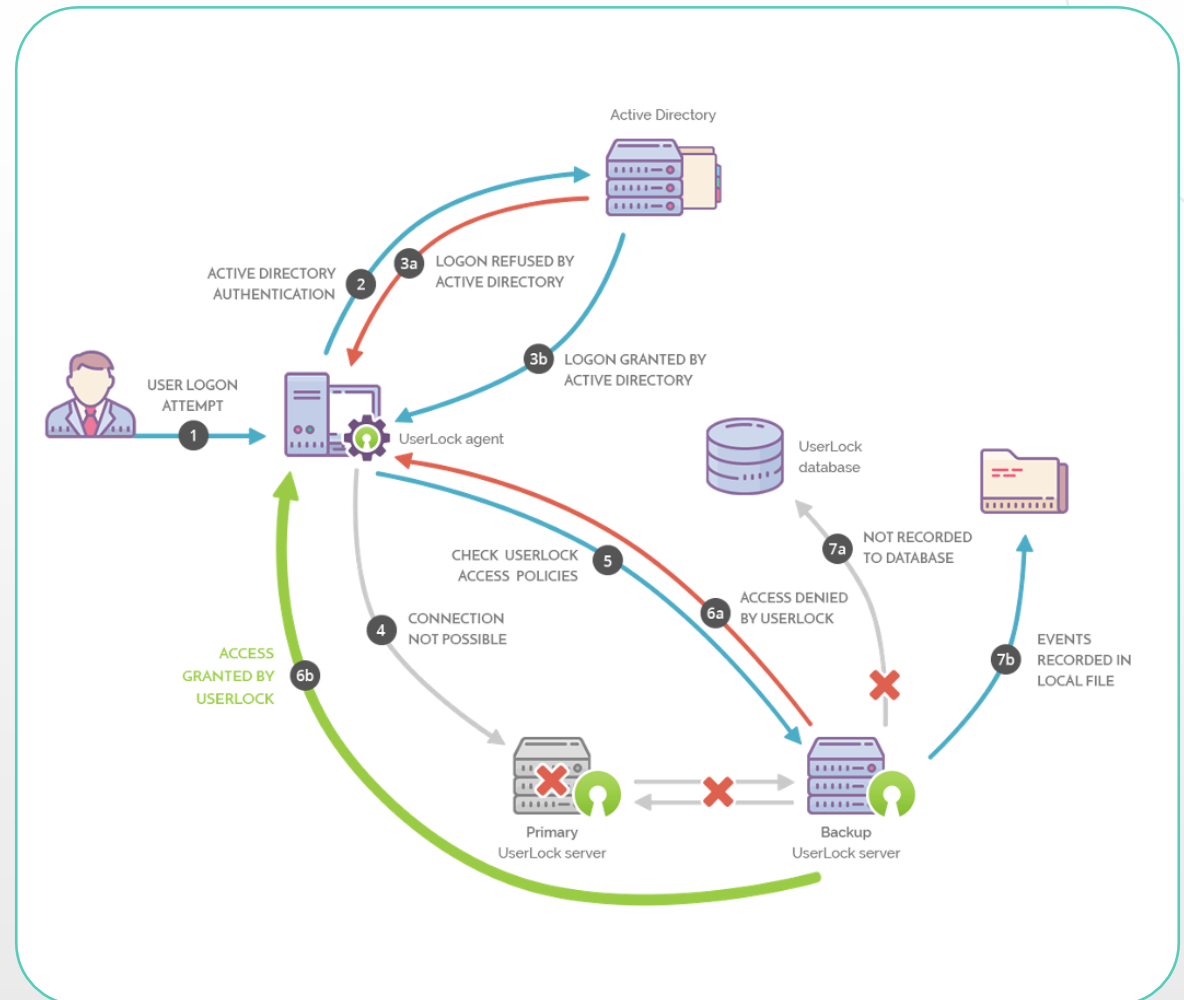
The server then communicates its decision to the agent regarding the acceptance or refusal of the connection requested.



How UserLock works in high availability

UserLock Backup Server

The **UserLock Backup Server** regularly synchronizes its configuration and its sessions database with the Primary server. If the Primary server has an issue, then the Backup server will automatically maintain the sessions activity monitoring and control of the network protected zone.



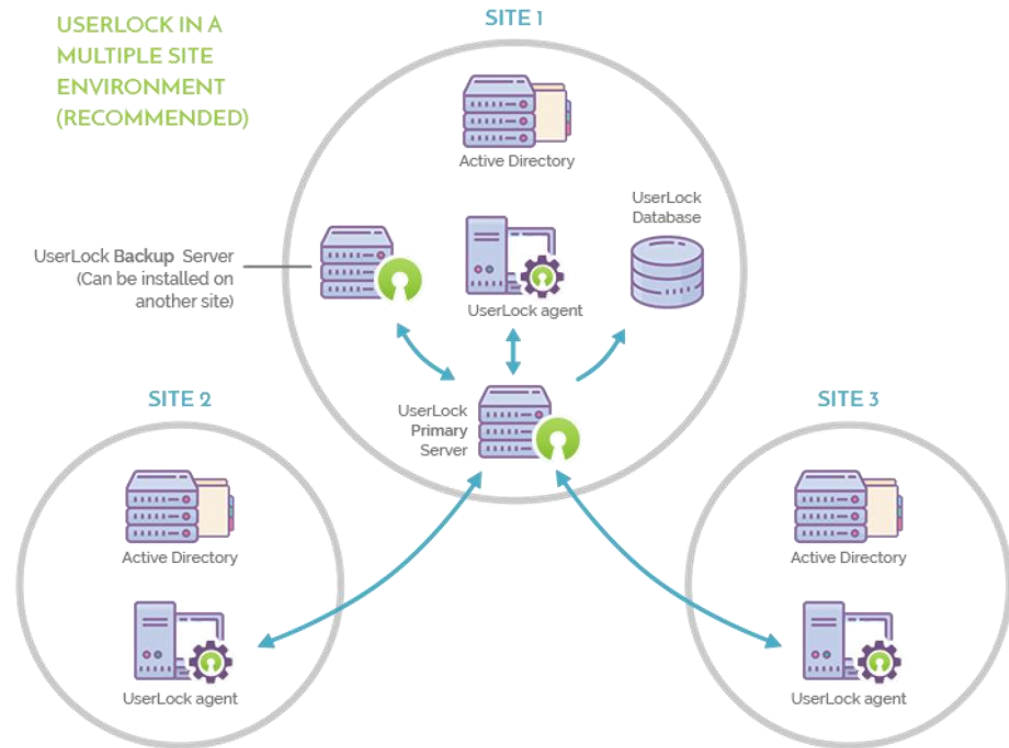
How UserLock works across multiple sites

It is possible to install UserLock to monitor multiple sites. The diagram shows how the agents installed on workstations will all contact the same UserLock service to allow for a centralized management.

UserLock service will contact the first available DC at the time of the user login.

If you would like to force the UserLock service to contact a specific DC, you can configure this in the advanced setting.

DcToContactForServerMember:



Recommended: Install the service on one server, and deploy the agent to end clients on all sites. This will allow you to manage all users in one centralized console.

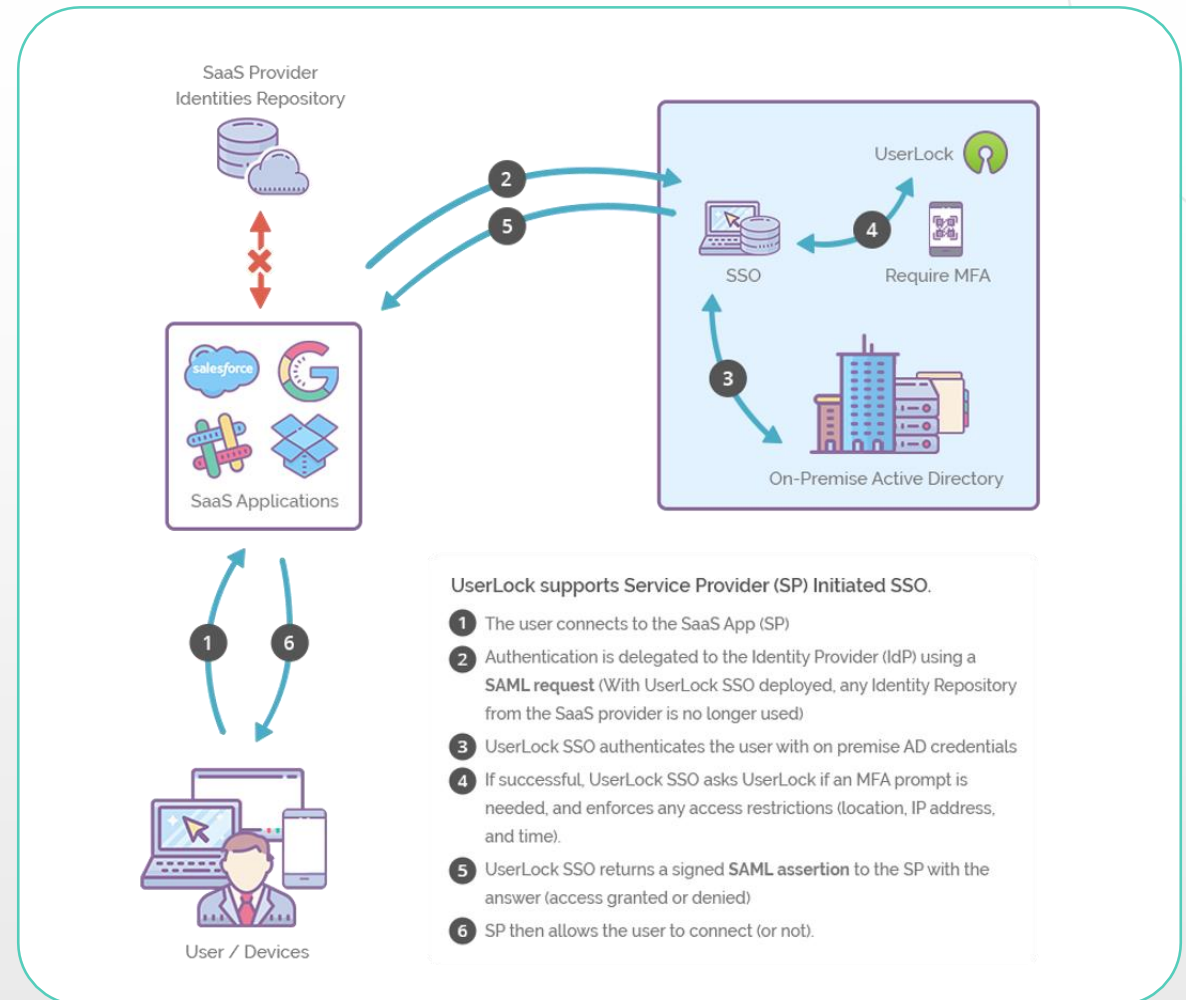
How UserLock single sign-on works

UserLock SSO for SaaS applications

UserLock SSO is hosted on premise and **retains Active Directory as the authoritative Identity Provider.**

For access to SaaS Applications, the user is authenticated with their **existing on premise credentials.**

Users may be prompted for **two-factor authentication**, depending on the conditions that are set.



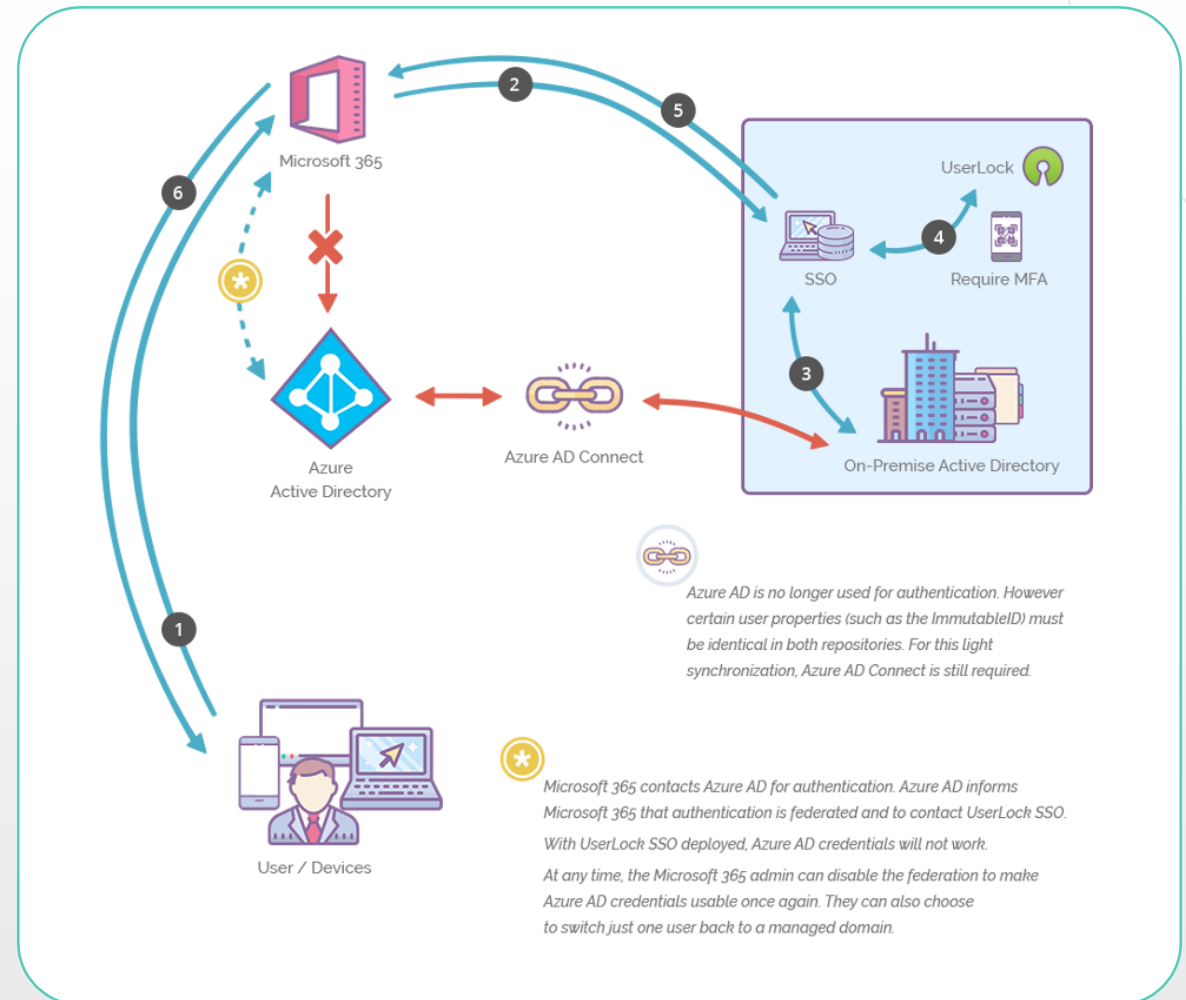
How UserLock single sign-on works

UserLock SSO for Microsoft 365

UserLock SSO is hosted on premise and **retains Active Directory as the authoritative Identity Provider**.

For access to Microsoft 365, the user is authenticated with their **existing on premise credentials**.

Users may be prompted for **two-factor authentication**, depending on the conditions that are set.



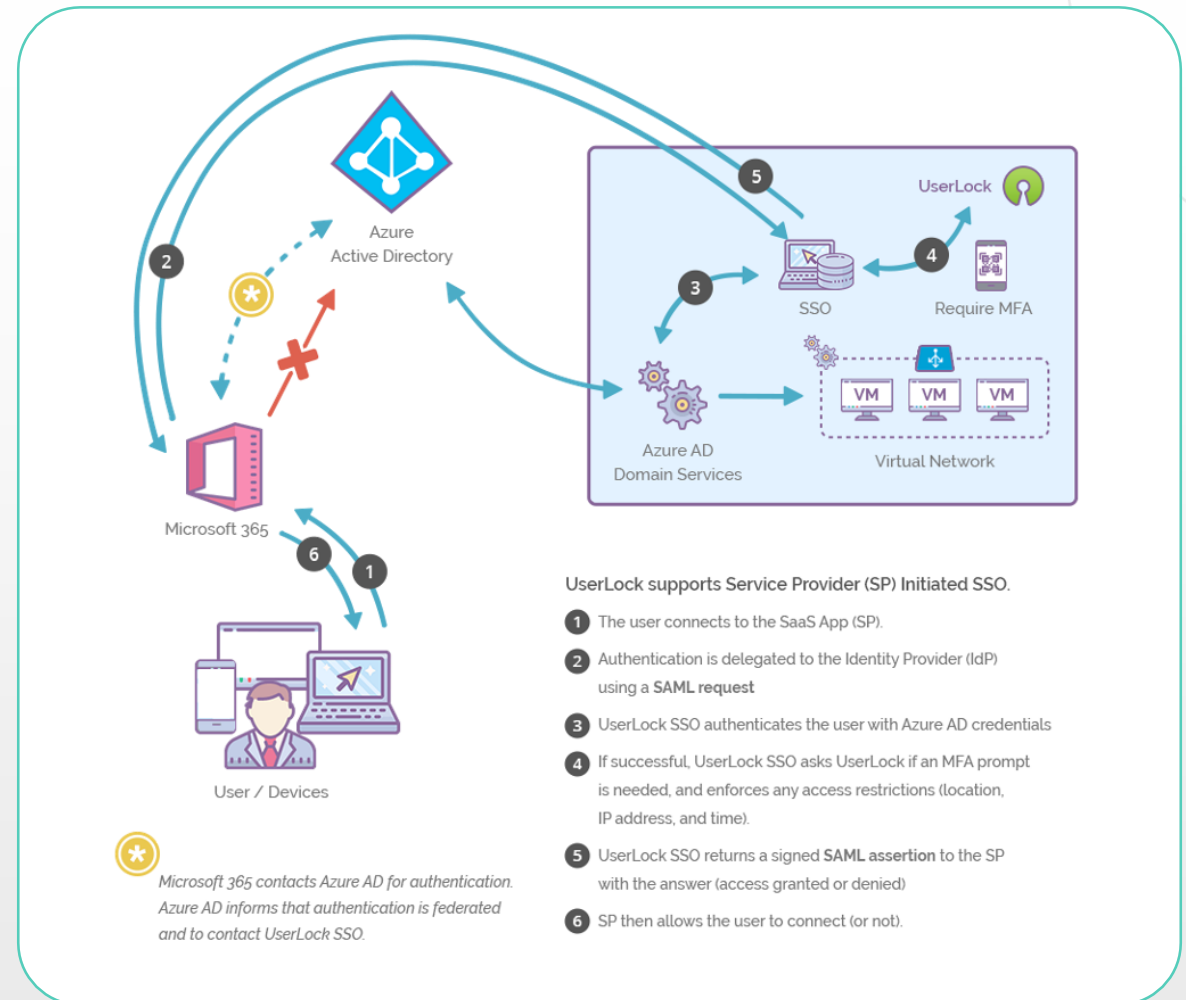
How UserLock single sign-on works

UserLock SSO for Microsoft 365 with Azure ad domain services

UserLock SSO can be hosted on a virtual network and **use Azure Active Directory as the authoritative Identity Provider**.

For access to SaaS Applications, the user is authenticated with their **Azure AD credentials**.

Users may be prompted for **two-factor authentication**, depending on the conditions that are set.



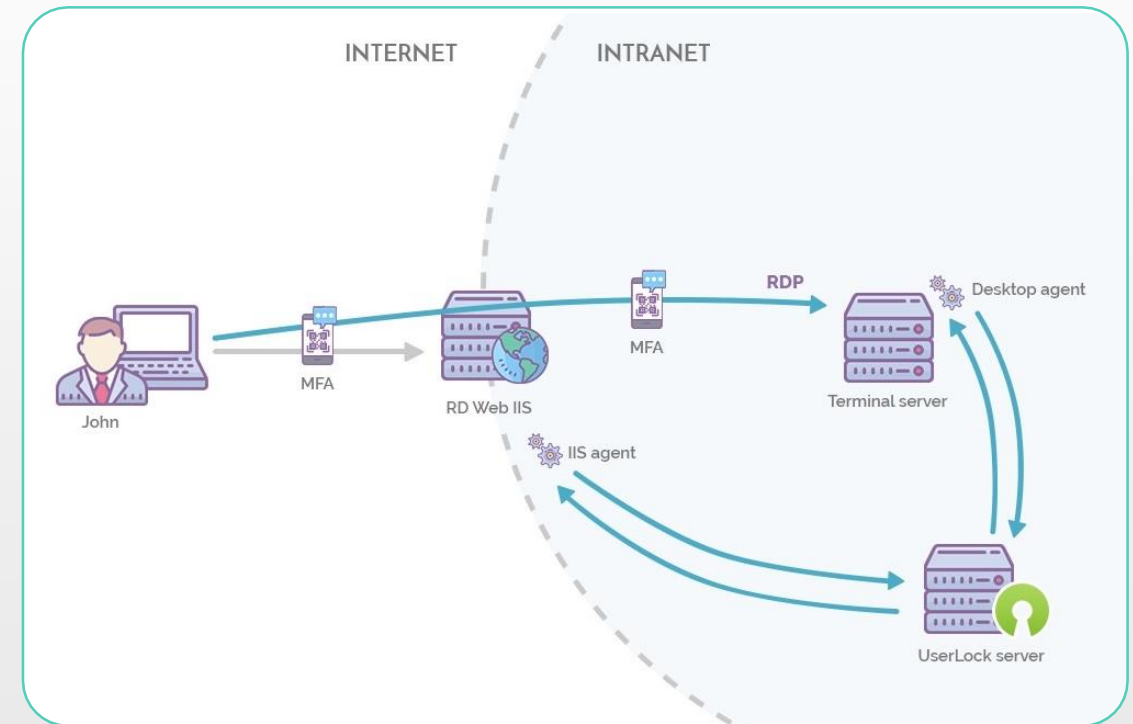
How UserLock secures RDP, RD Gateway, and RD Web

MFA

Apply MFA granularly on the RD Web connection, RDP, or both. Specify whether every MFA connection passing through the RD Gateway should require an authentication prompt, or only those originating outside the network.

Access controls

Set access restrictions based on user, group, or OU. Allows for role-based access policies following the principle of least privilege and streamlined change management. Limit concurrent sessions to minimize brute force and session hijack attacks. Limit remote access based on geolocation, IP address, device, or workstation.



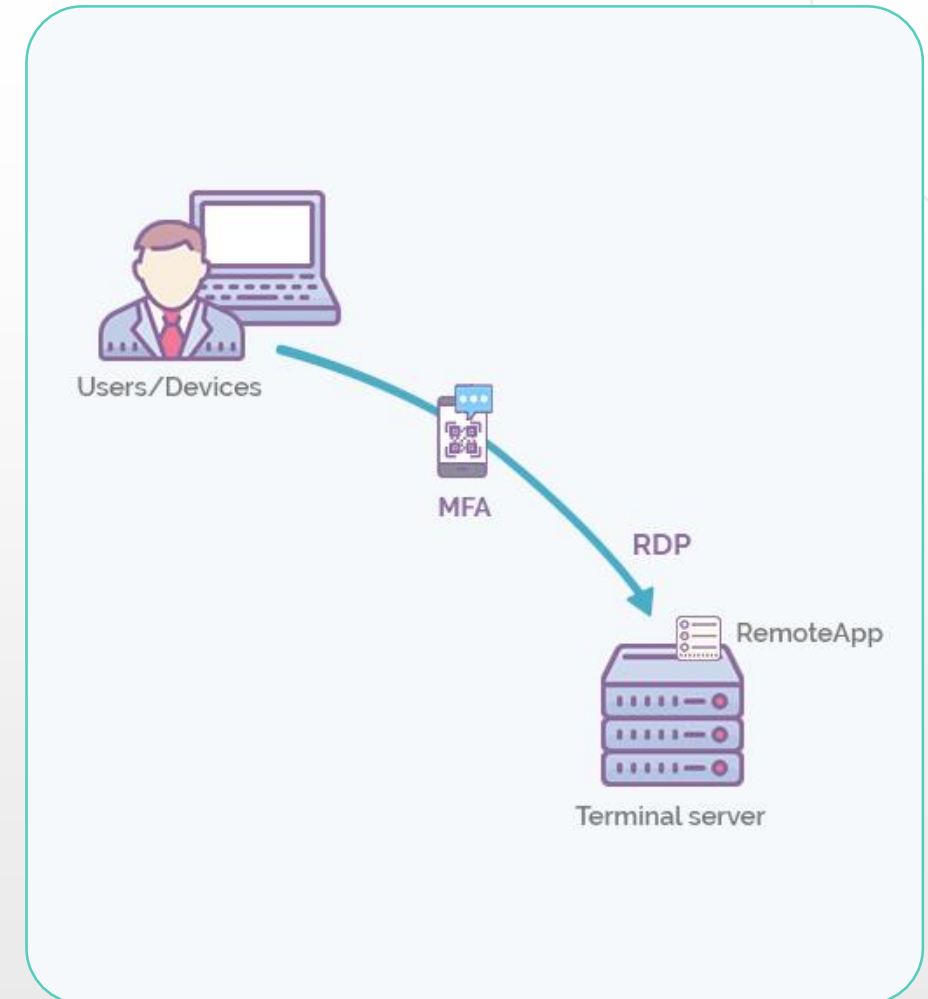
How UserLock secures RemoteApp access

MFA

Apply MFA to all RemoteApp sessions, whether the user connects via RD Web or opens the RemoteApp directly from their desktop.

Access controls

Set access restrictions based on user, group, or OU. Allows for role-based access policies following the principle of least-privilege and streamlined change management. Limit concurrent sessions to minimize brute force and session hijack attacks. Limit RemoteApp access based on geolocation, IP address, device, or workstation.



How UserLock protects Outlook on the Web Access (OWA)

MFA

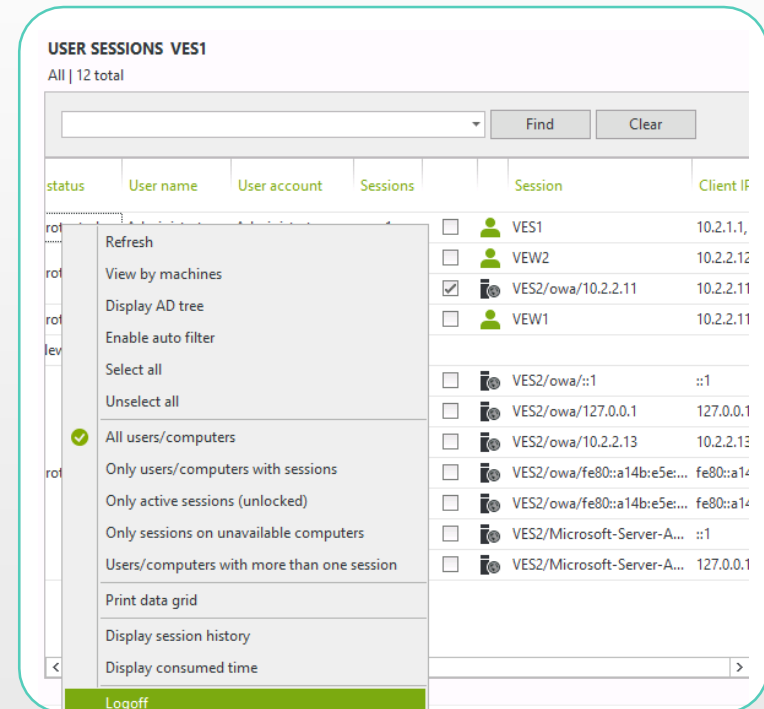
When you install UserLock, the MFA agent for OWA is installed on the existing IIS server. You can control when to prompt for MFA, based on: time of day, device location, and AD user, group, and OU.

Access controls

Restrict mailbox access by IP address.

Detect unauthorized mailbox access

Detect if one of your users tries to log onto another user's mailbox, and click logoff to close the suspicious session.



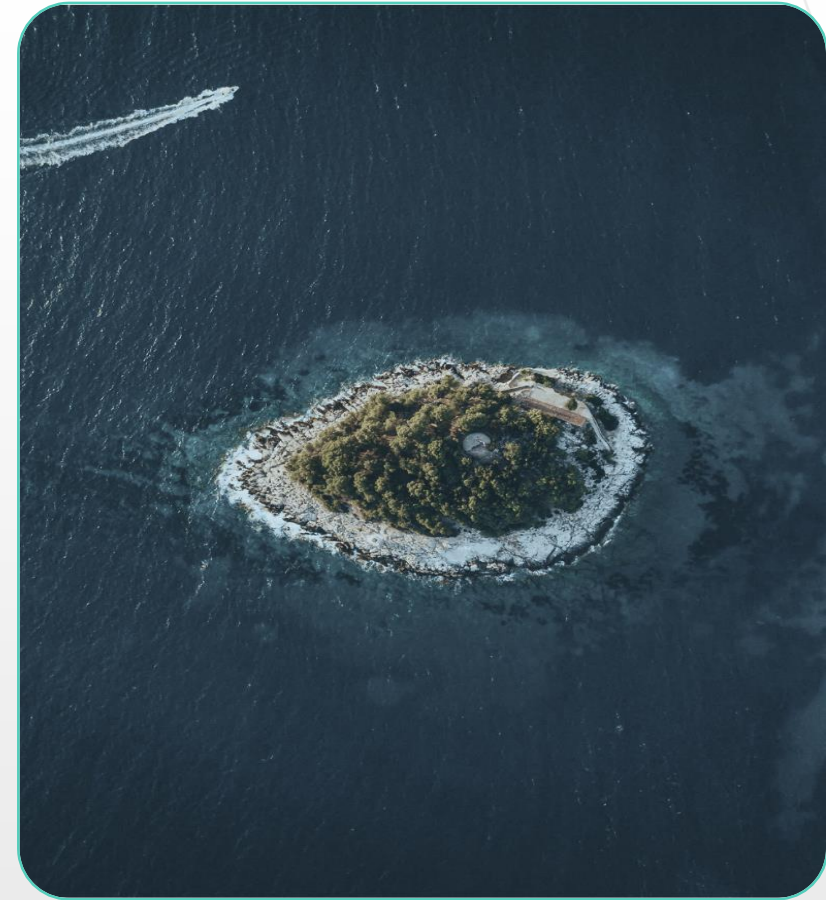
How UserLock secures air-gapped environments

MFA

Apply MFA on AD identity access to your air-gapped network using HOTP tokens, TOTP with a programmable token or authenticator app, or push notifications with UserLock Push.

Access controls

Limit the scope for insider attacks with access restrictions based on time, geolocation, workstation, or AD user, group or OU. Limit concurrent sessions to reduce the risk of unauthorized access. Get real-time monitoring and alerts, and audit and report on MFA events, session history, and user access (or attempted access) to your air-gapped environment.



IS Decisions®