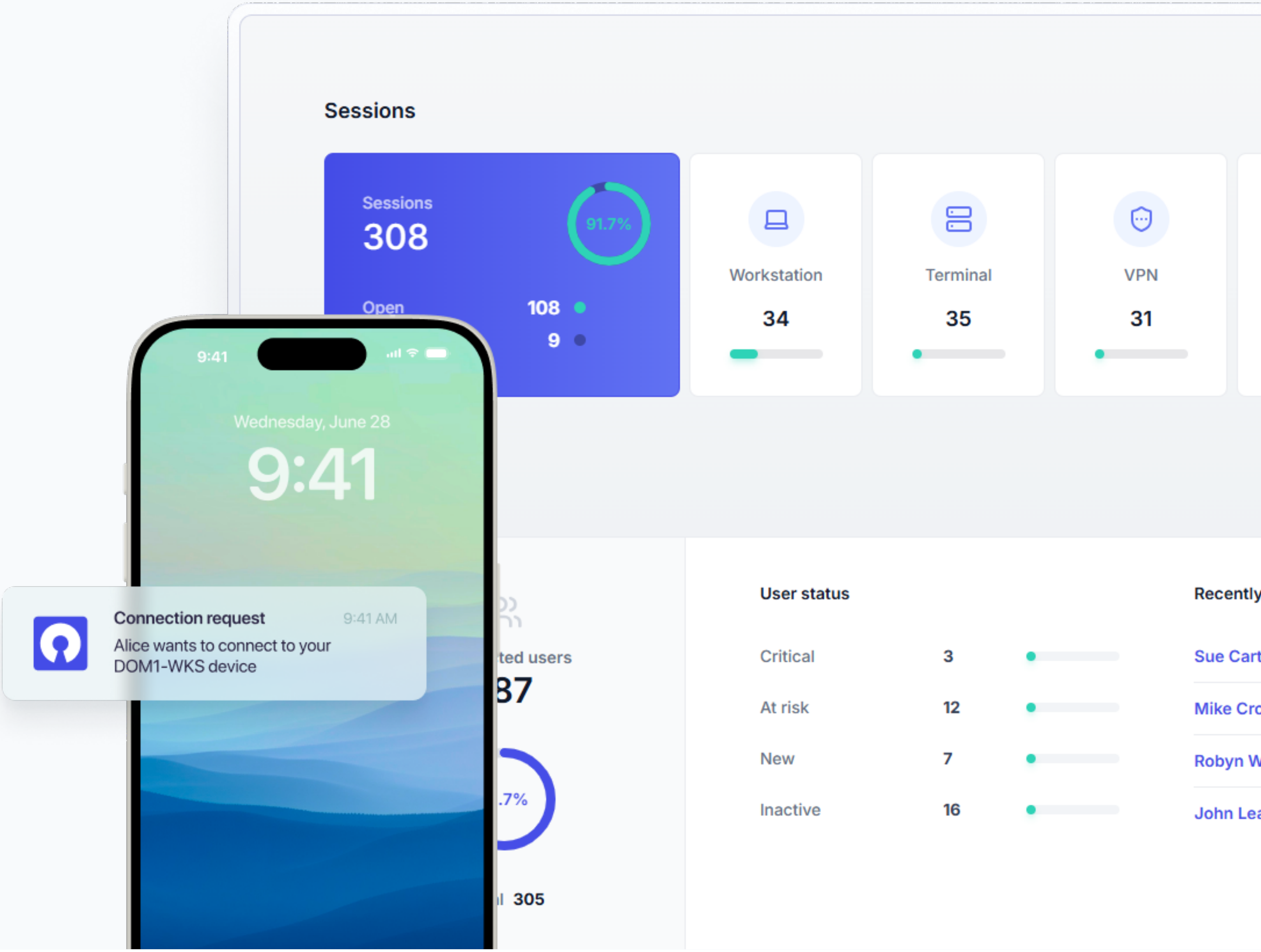
USERLOCK

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



Connection request 9:41 AM

Alice wants to connect to your DOM1-WKS device

Sessions

Sessions	Workstation	Terminal	VPN
308	34	35	31

Open 108

9

User status

		Recently
Critical	3	Sue Cart
At risk	12	Mike Cro
New	7	Robyn W
Inactive	16	John Lea

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.

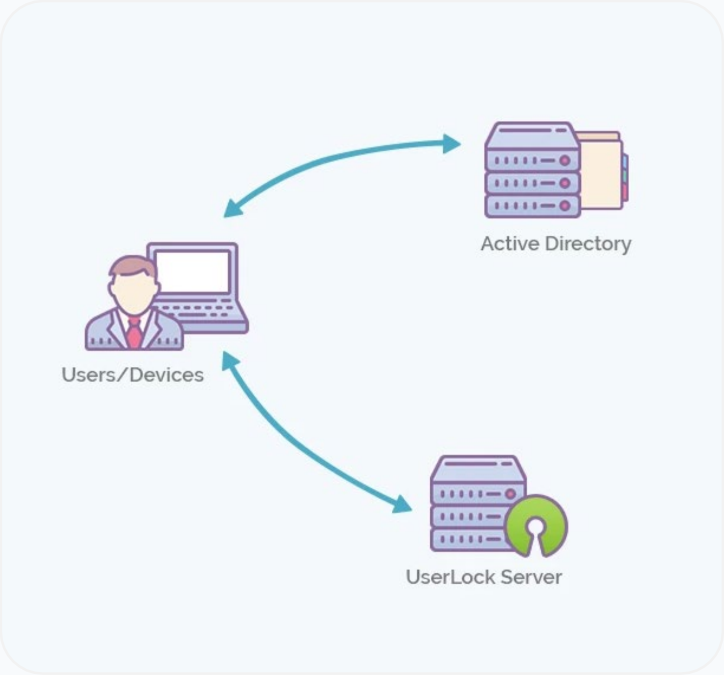
HIGH POINT NETWORKS
matrix IT SUPPORT
EuskoData Soluciones Tecnológicas
angliss HONG KONG
ZOODFOOD
COASTAL Housing Group
MICHIGAN STATE UNIVERSITY
City School District of ALBANY
NORTHERN LIGHTS
DEPARTMENT OF JUSTICE
Ministerie van Defensie
TURKISH AEROSPACE
trois-rivières
KEIZER SINCE 1982
LA MAYENNE Le Département
NEW YORK CITY COLLEGE OF TECHNOLOGY CITY TECH
University of Kent
CAMDEN CITY SCHOOL DISTRICT
Oklahoma City PUBLIC SCHOOLS
Santander
FIS
بنك بوبيان Boubyan Bank
Star Union Dai-ichi LIFE INSURANCE
MOORE CAPITAL
First Flight FEDERAL CREDIT UNION
arnold IMMOBILIEN
LINEMASTER
Peterbilt DOBBS PETERBILT
EUROCONTROLLI
MRIoA
Clemson Eye
NHS
ANEW
DUBAI LONDON CLINIC
sabin MEDICINA DIAGNÓSTICA
DP WORLD
OTOLIFT MONTE-ESCALIERS
Rieckermann Machinery & Industrial Solutions

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



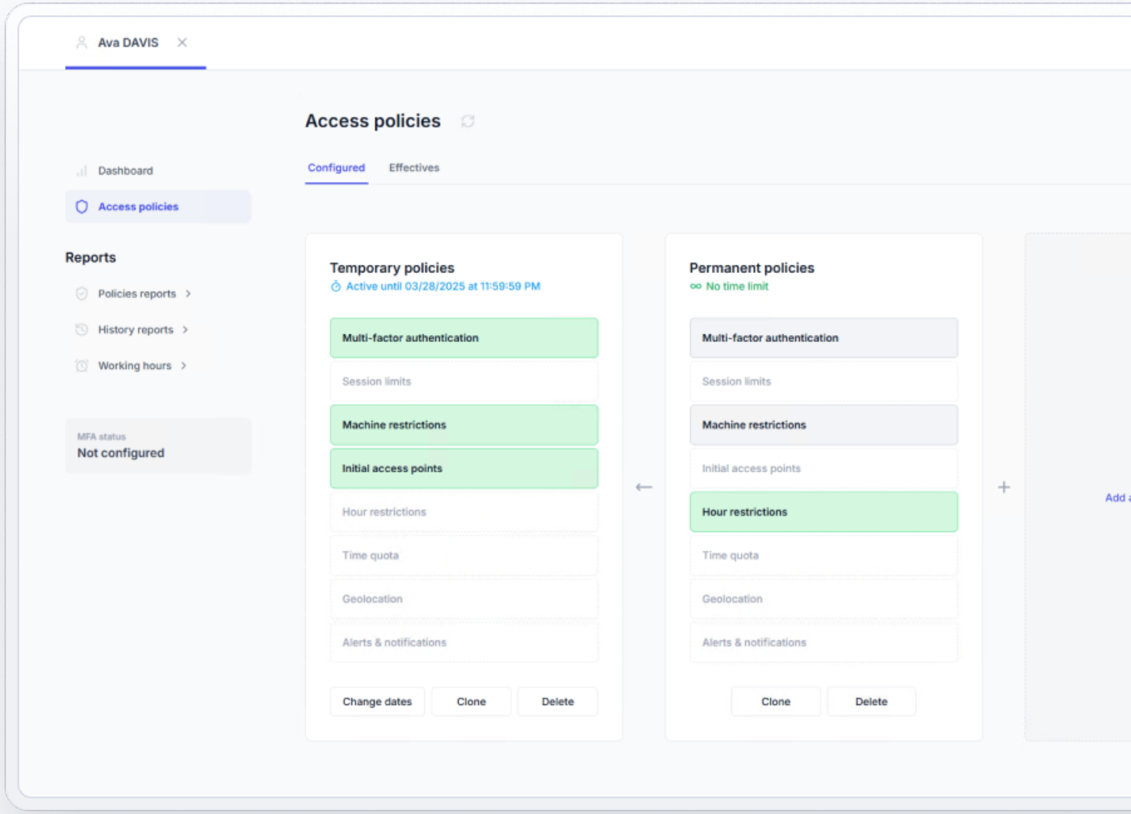
UserLock closes common access security gaps

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



MFA status
Not configured

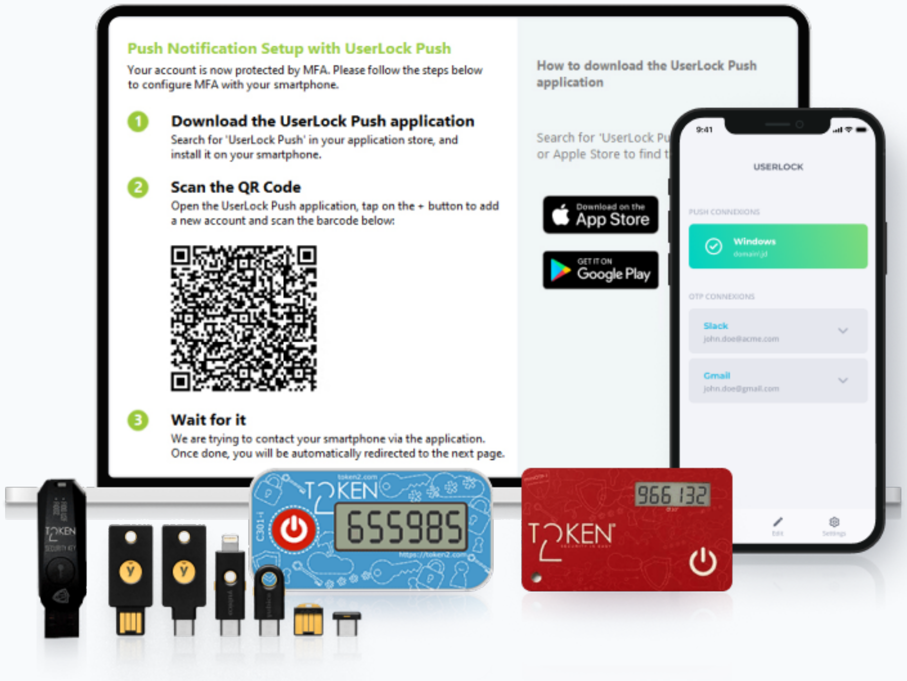
Active until 03/28/2025 at 11:59:59 PM

No time limit

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.



Push Notification Setup with UserLock Push

Your account is now protected by MFA. Please follow the steps below to configure MFA with your smartphone.

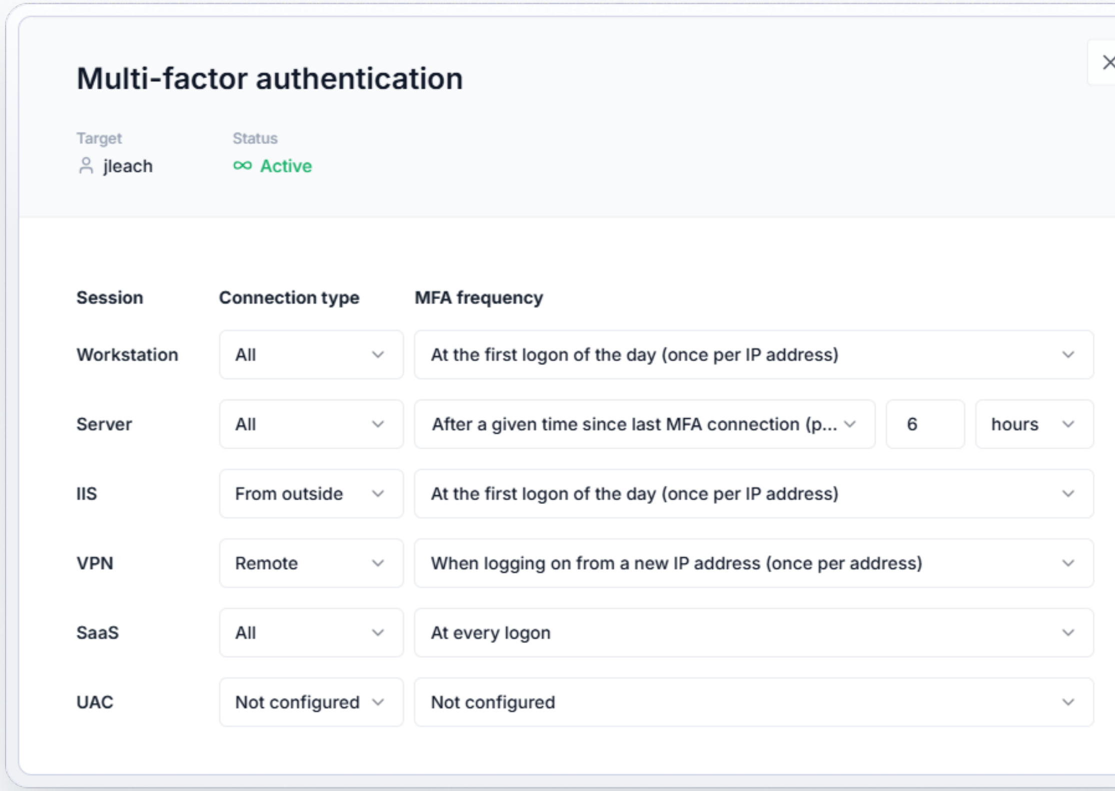
1. Download the UserLock Push application
   Search for 'UserLock Push' in your application store, and install it on your smartphone.
2. Scan the QR Code
   Open the UserLock Push application, tap on the + button to add a new account and scan the barcode below:
3. Wait for it
   We are trying to contact your smartphone via the application. Once done, you will be automatically redirected to the next page.

How to download the UserLock Push application

Search for 'UserLock Pu
or Apple Store to find t

Customized MFA

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



Multi-factor authentication

Target
jleach

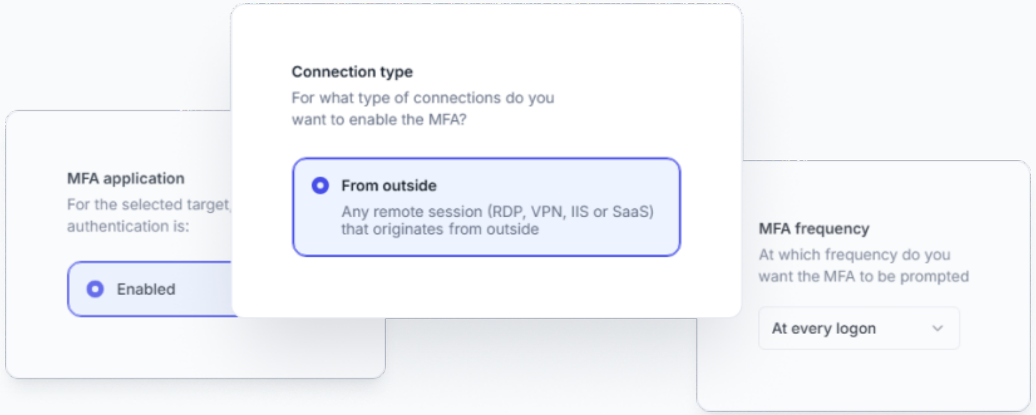
Status
∞ Active

Session	Connection type	MFA frequency
Workstation	All	At the first logon of the day (once per IP address)
Server	All	After a given time since last MFA connection (p... 6 hours
IIS	From outside	At the first logon of the day (once per IP address)
VPN	Remote	When logging on from a new IP address (once per address)
SaaS	All	At every logon
UAC	Not configured	Not configured

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.



MFA application

For the selected target, authentication is:

● Enabled

Connection type

For what type of connections do you want to enable the MFA?

● **From outside**
Any remote session (RDP, VPN, IIS or SaaS) that originates from outside

MFA frequency

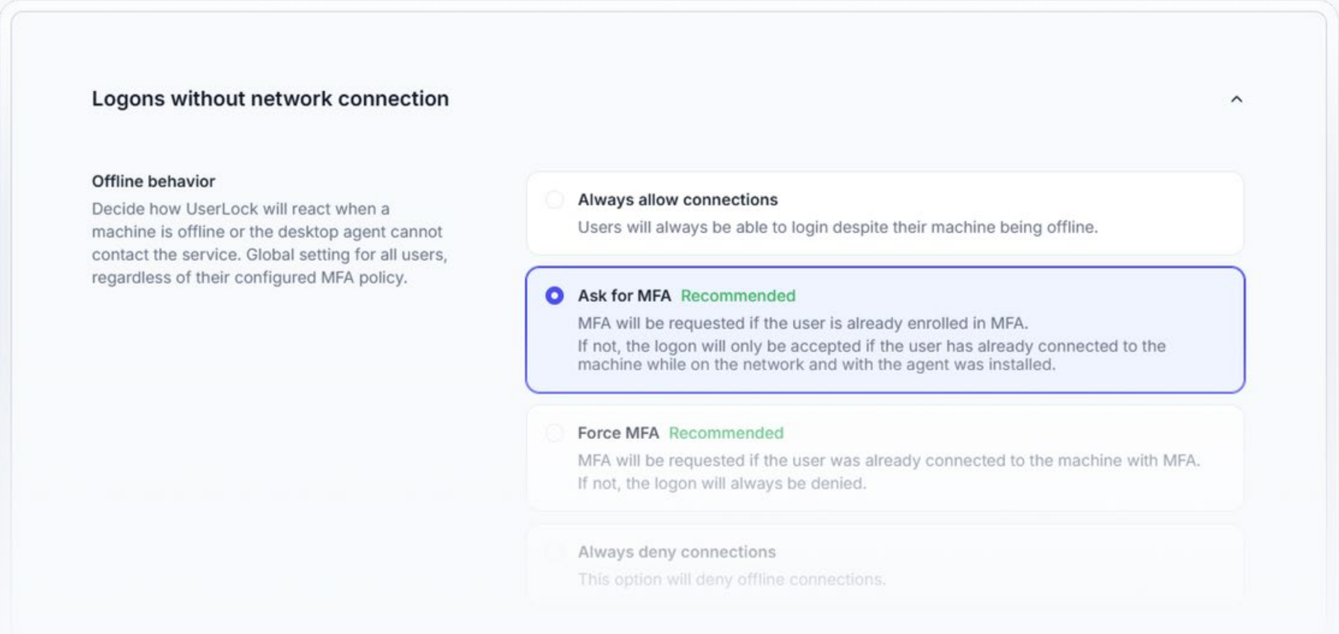
At which frequency do you want the MFA to be prompted

At every logon

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.



Logons without network connection

Offline behavior
Decide how UserLock will react when a machine is offline or the desktop agent cannot contact the service. Global setting for all users, regardless of their configured MFA policy.

○ **Always allow connections**
Users will always be able to login despite their machine being offline.

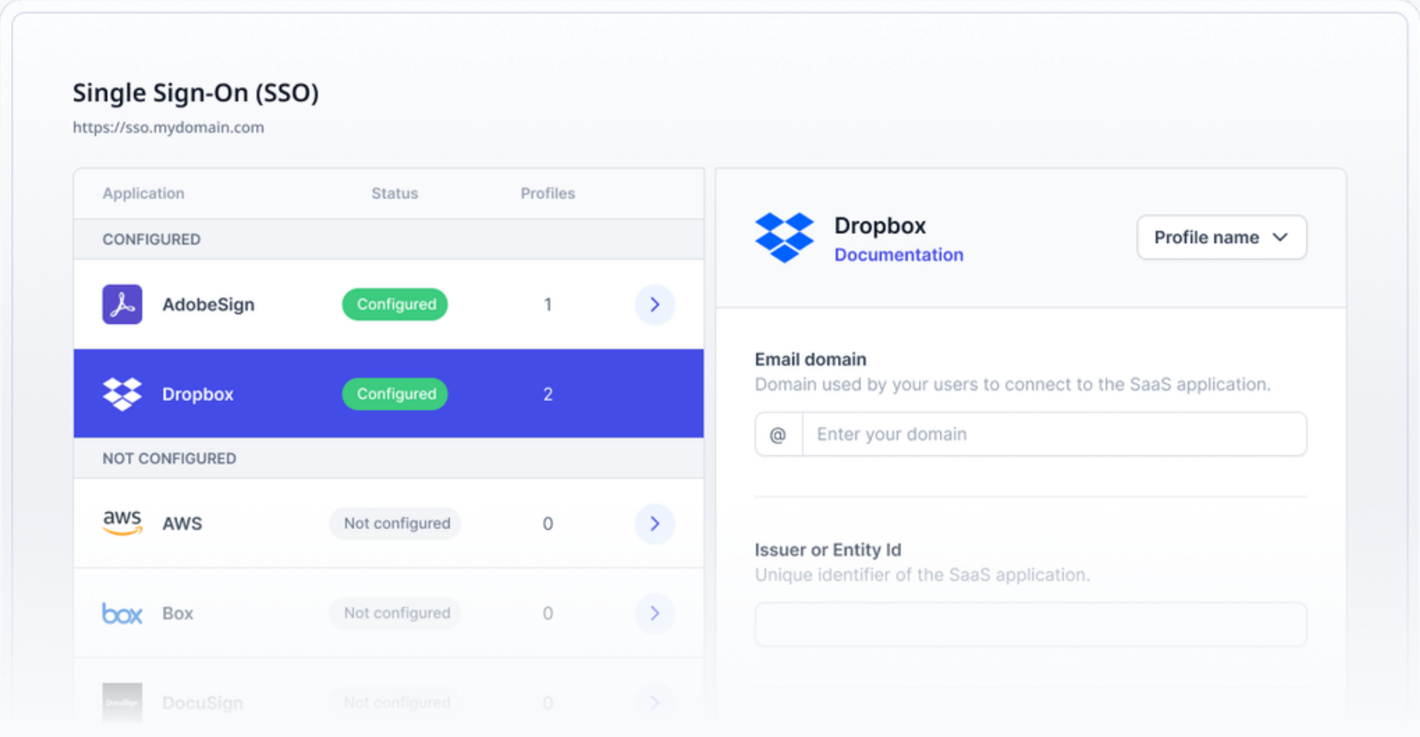
● **Ask for MFA** Recommended
MFA will be requested if the user is already enrolled in MFA.
If not, the logon will only be accepted if the user has already connected to the machine while on the network and with the agent was installed.

○ **Force MFA** Recommended
MFA will be requested if the user was already connected to the machine with MFA.
If not, the logon will always be denied.

○ Always deny connections
This option will deny offline connections.

Single sign-on

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



Single Sign-On (SSO)

https://sso.mydomain.com

Application	Status	Profiles
CONFIGURED		
AdobeSign	Configured	1
Dropbox	Configured	2
NOT CONFIGURED		
AWS	Not configured	0
Box	Not configured	0
DocuSign	Not configured	0

Dropbox

Documentation

Profile name

Email domain

Domain used by your users to connect to the SaaS application.

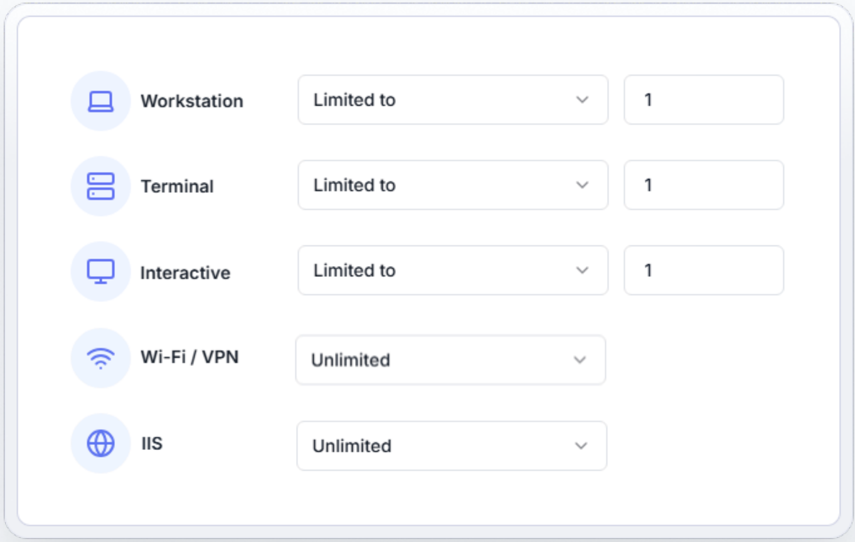
@ Enter your domain

Issuer or Entity Id

Unique identifier of the SaaS application.

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.

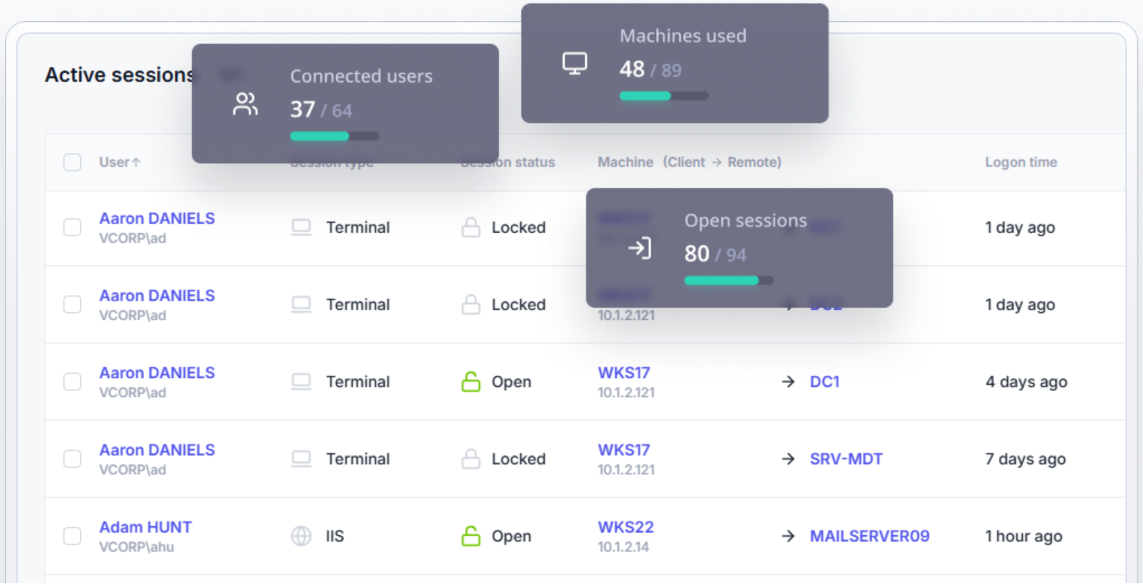


Workstation	Limited to	1
Terminal	Limited to	1
Interactive	Limited to	1
Wi-Fi / VPN	Unlimited	
IIS	Unlimited	

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.



Active sessions

Connected users 37 / 64

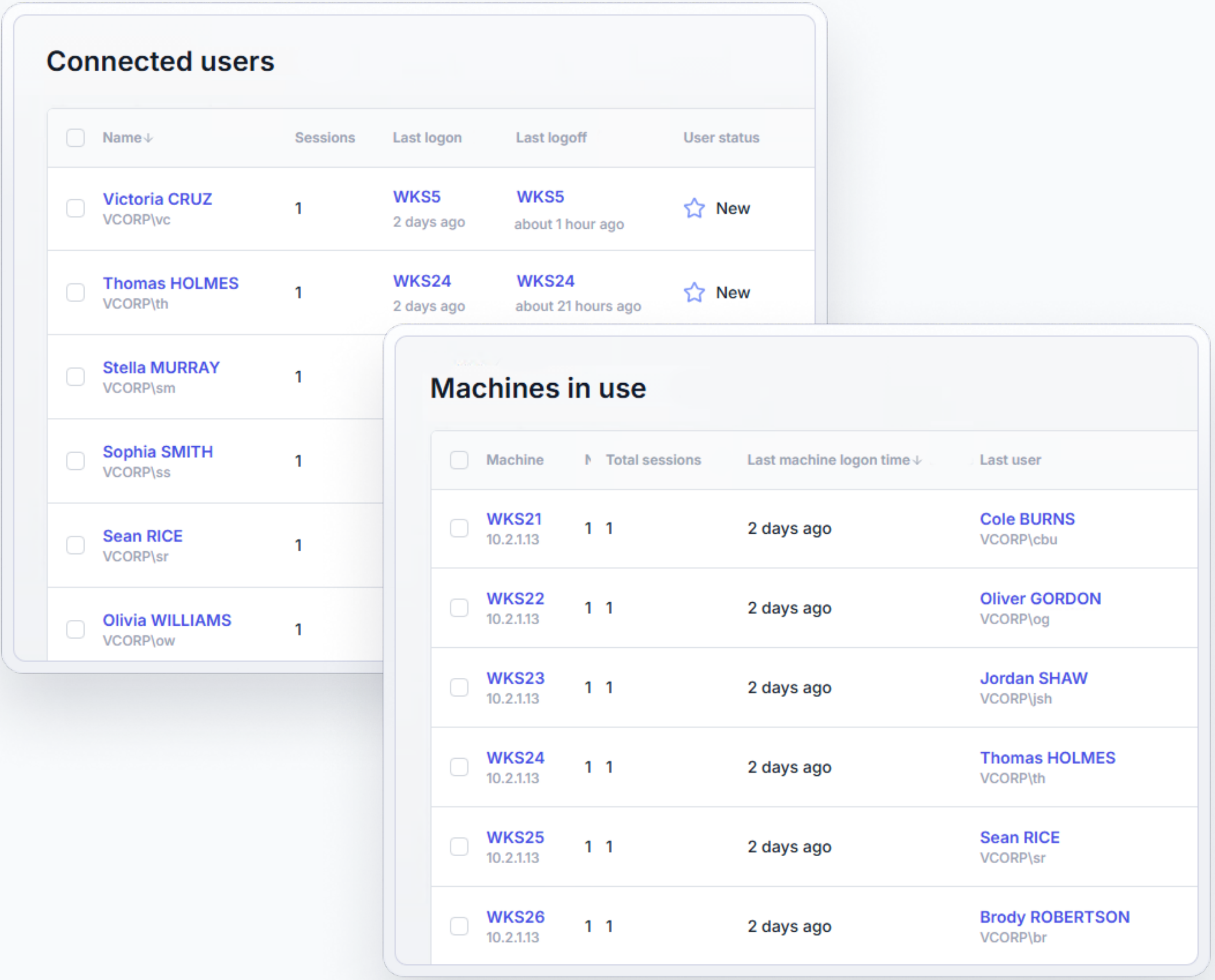
Machines used 48 / 89

Open sessions 80 / 94

□	User↑	Session type	Session status	Machine (Client → Remote)		Logon time
□	Aaron DANIELS VCORP\ad	Terminal	Locked	[illegible]	[illegible]	1 day ago
□	Aaron DANIELS VCORP\ad	Terminal	Locked	[illegible] 10.1.2.121	→ [illegible]	1 day ago
□	Aaron DANIELS VCORP\ad	Terminal	Open	WKS17 10.1.2.121	→ DC1	4 days ago
□	Aaron DANIELS VCORP\ad	Terminal	Locked	WKS17 10.1.2.121	→ SRV-MDT	7 days ago
□	Adam HUNT VCORP\ahu	IIS	Open	WKS22 10.1.2.14	→ MAILSERVER09	1 hour ago

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.



Connected users

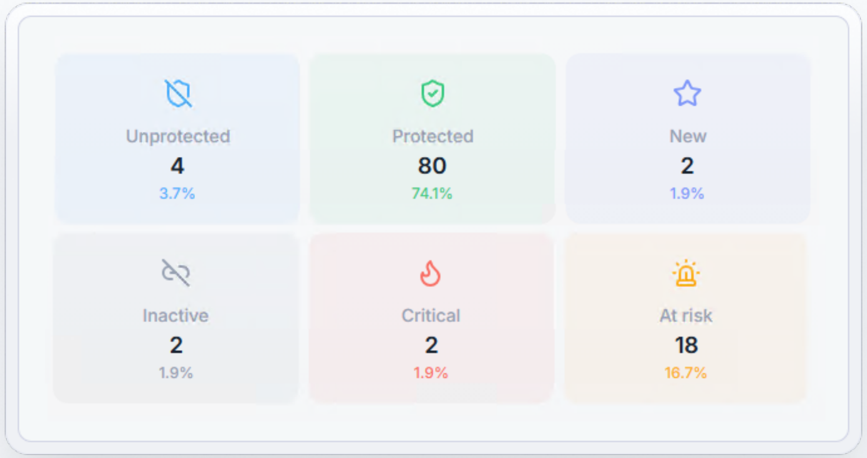
□	Name↓	Sessions	Last logon	Last logoff	User status
□	Victoria CRUZ VCORP\vc	1	WKS5 2 days ago	WKS5 about 1 hour ago	☆ New
□	Thomas HOLMES VCORP\th	1	WKS24 2 days ago	WKS24 about 21 hours ago	☆ New
□	Stella MURRAY VCORP\sm	1			
□	Sophia SMITH VCORP\ss	1			
□	Sean RICE VCORP\sr	1			
□	Olivia WILLIAMS VCORP\ow	1			

Machines in use

□	Machine	N	Total sessions	Last machine logon time↓	Last user
□	WKS21 10.2.1.13	1	1	2 days ago	Cole BURNS VCORP\cbu
□	WKS22 10.2.1.13	1	1	2 days ago	Oliver GORDON VCORP\og
□	WKS23 10.2.1.13	1	1	2 days ago	Jordan SHAW VCORP\jsh
□	WKS24 10.2.1.13	1	1	2 days ago	Thomas HOLMES VCORP\th
□	WKS25 10.2.1.13	1	1	2 days ago	Sean RICE VCORP\sr
□	WKS26 10.2.1.13	1	1	2 days ago	Brody ROBERTSON VCORP\br

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



Unprotected 4 3.7%	Protected 80 74.1%	New 2 1.9%
Inactive 2 1.9%	Critical 2 1.9%	At risk 18 16.7%

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.

Multi-factor authentication

How does MFA help prevent ransomware?

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

Peterbilt | DOBBS PETERBILT

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.

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 Infastructure 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

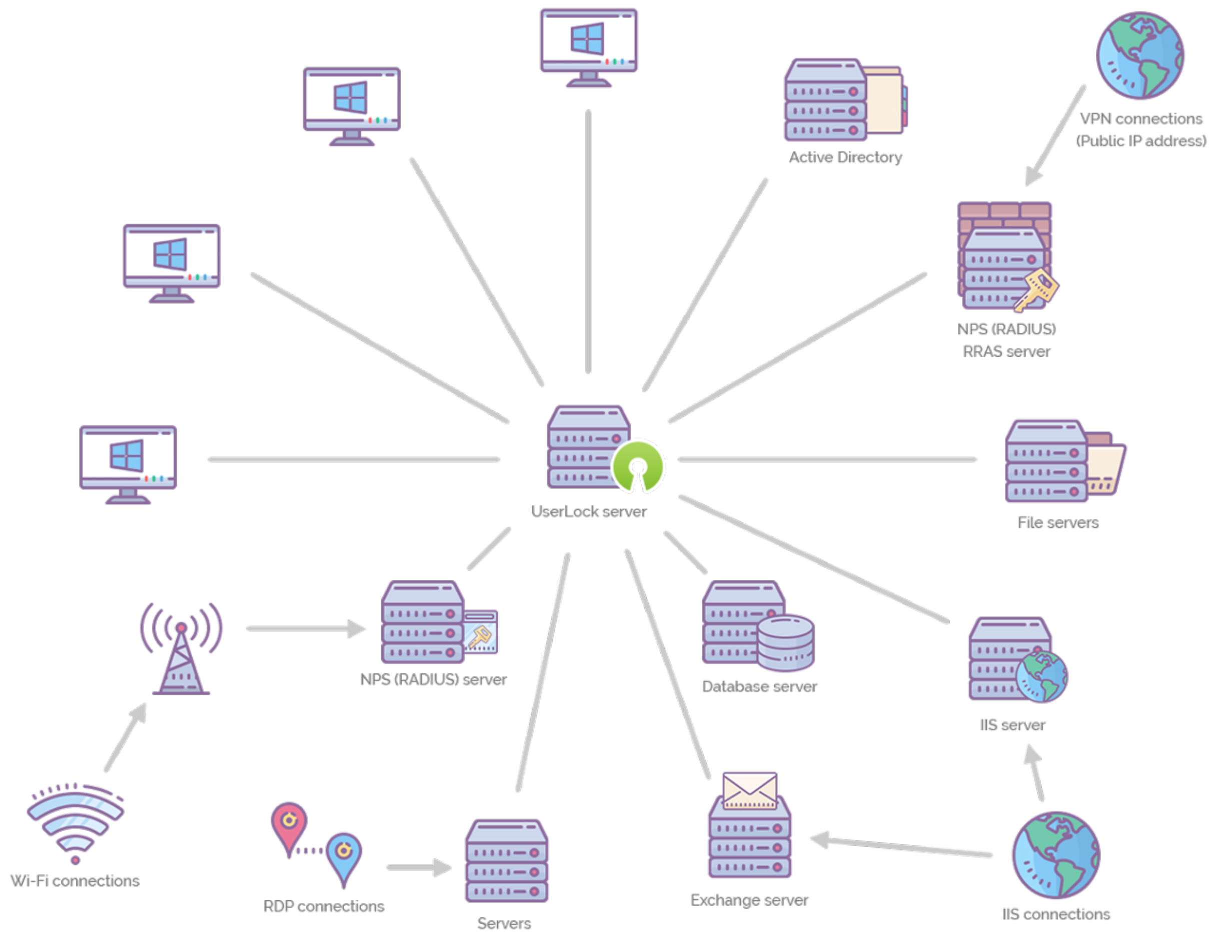
Senior IT Project Manager in Professional Services, United States

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

IT SECURITY GURU
THE SITE FOR OUR COMMUNITY

Infrastructure

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

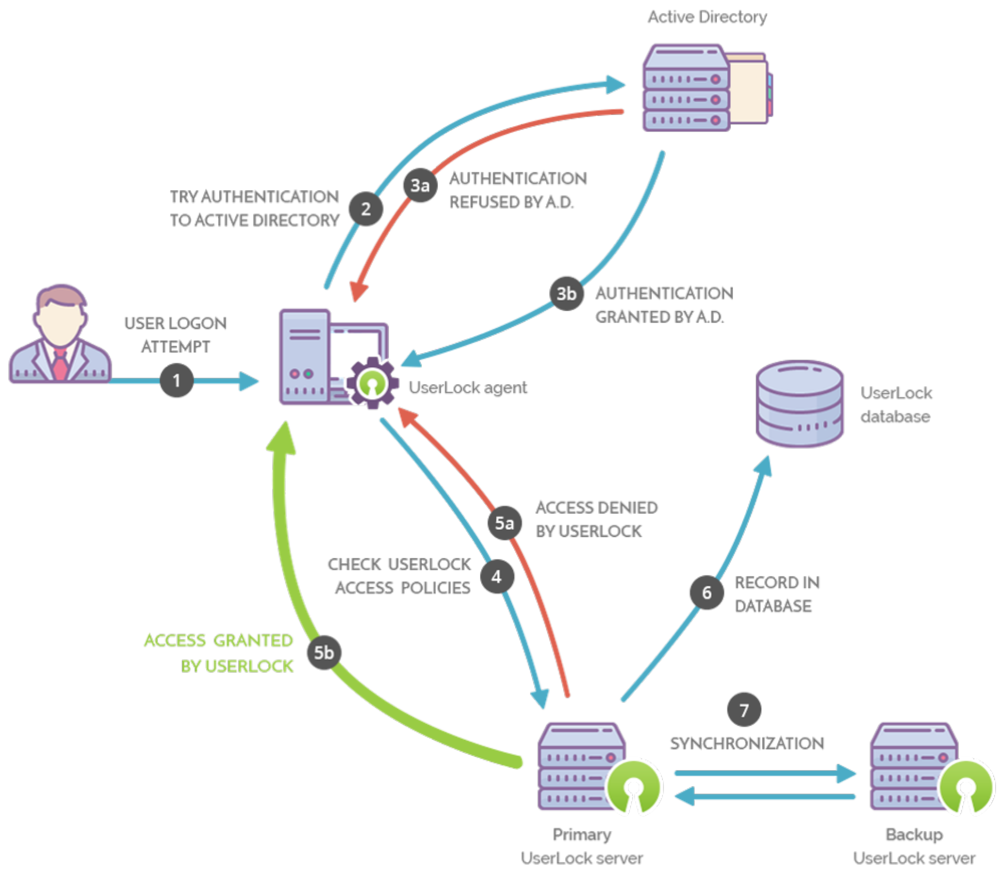


How UserLock works

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.


Active Directory
TRY AUTHENTICATION TO ACTIVE DIRECTORY
2
3a
AUTHENTICATION REFUSED BY A.D.
3b
AUTHENTICATION GRANTED BY A.D.
USER LOGON ATTEMPT
1
UserLock agent
UserLock database
5a
ACCESS DENIED BY USERLOCK
CHECK USERLOCK ACCESS POLICIES
4
6
RECORD IN DATABASE
ACCESS GRANTED BY USERLOCK
5b
7
SYNCHRONIZATION
Primary UserLock server
Backup UserLock server

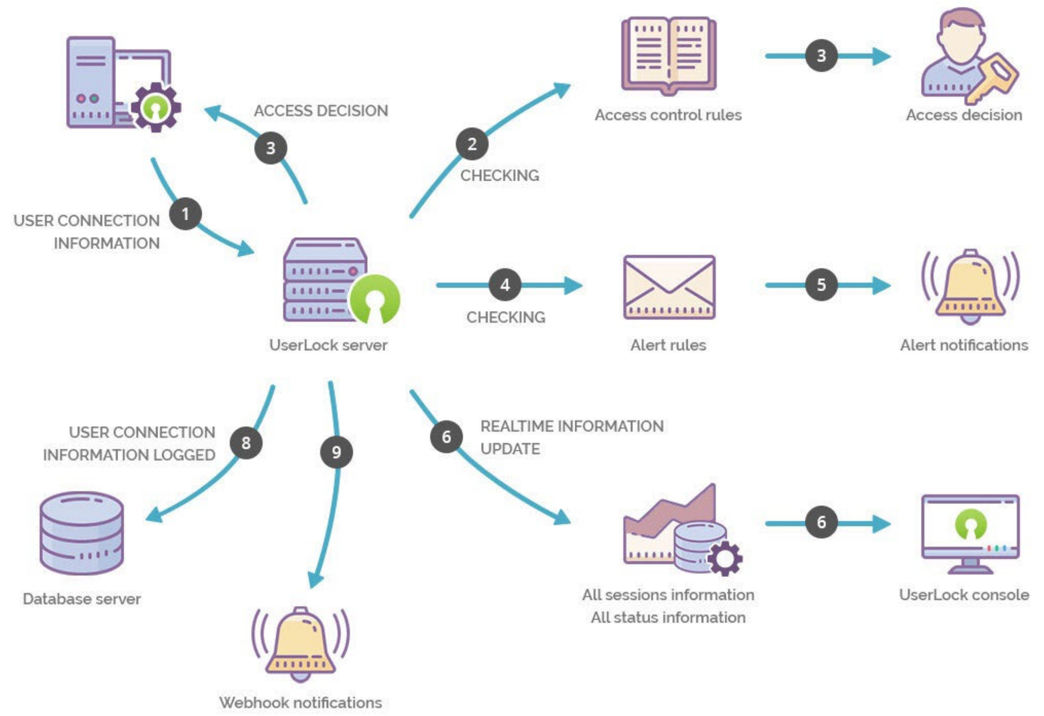
How UserLock works

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.

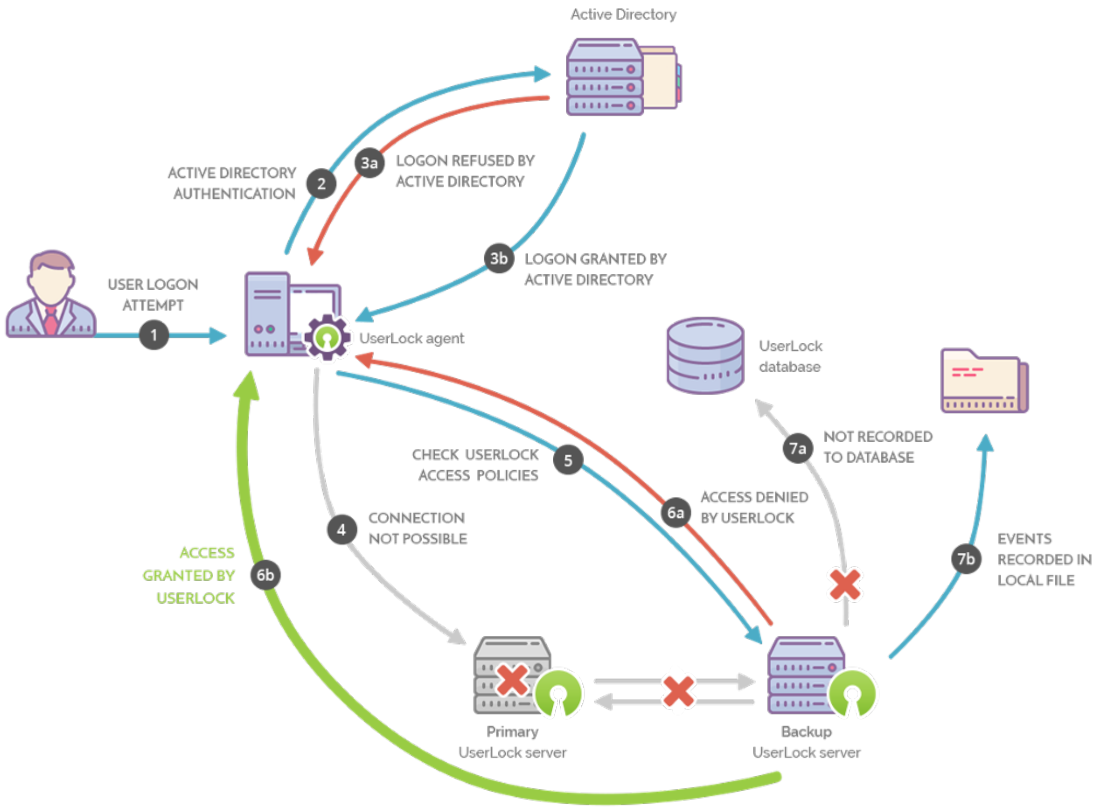
The server then communicates its decision to the agent regarding the acceptance or refusal of the connection requested.



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.


Active Directory
ACTIVE DIRECTORY AUTHENTICATION
2
3a
LOGON REFUSED BY ACTIVE DIRECTORY
3b
LOGON GRANTED BY ACTIVE DIRECTORY
USER LOGON ATTEMPT
1
UserLock agent
UserLock database
CHECK USERLOCK ACCESS POLICIES
5
7a
NOT RECORDED TO DATABASE
6a
ACCESS DENIED BY USERLOCK
4
CONNECTION NOT POSSIBLE
ACCESS GRANTED BY USERLOCK
6b
7b
EVENTS RECORDED IN LOCAL FILE
Primary UserLock server
Backup UserLock server

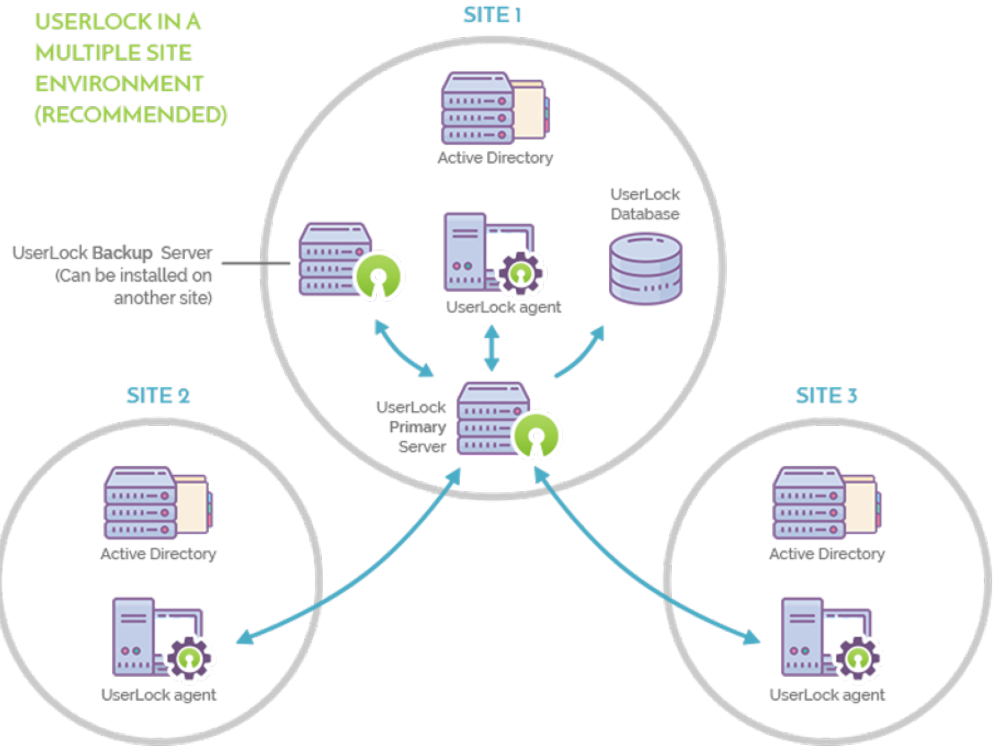
How UserLock works across multiple sites

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.

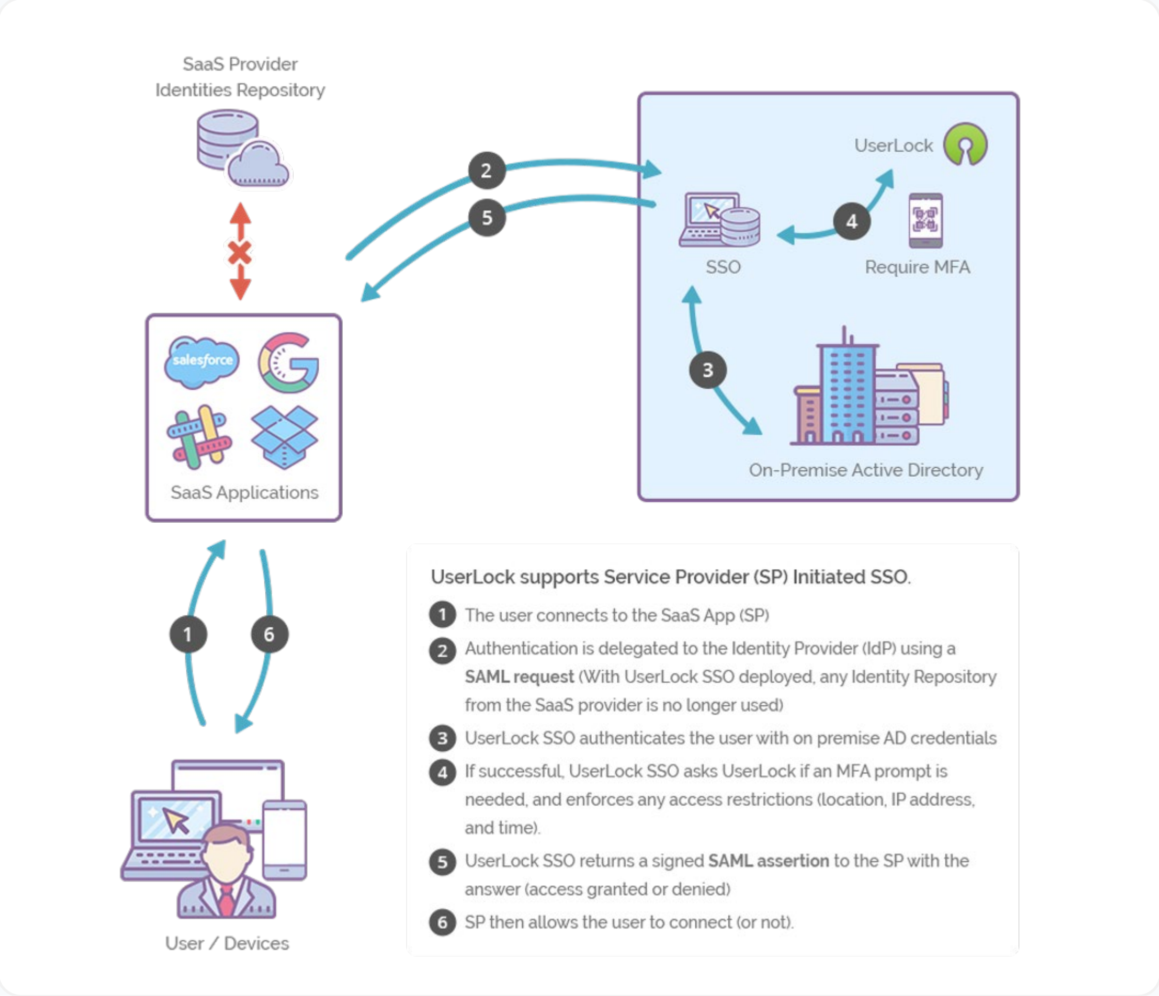
How UserLock single sign-on works

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.



UserLock supports Service Provider (SP) Initiated SSO.

1. The user connects to the SaaS App (SP)
2. Authentication is delegated to the Identity Provider (IdP) using a **SAML request** (With UserLock SSO deployed, any Identity Repository from the SaaS provider is no longer used)
3. UserLock SSO authenticates the user with on premise AD credentials
4. If successful, UserLock SSO asks UserLock if an MFA prompt is needed, and enforces any access restrictions (location, IP address, and time).
5. UserLock SSO returns a signed **SAML assertion** to the SP with the answer (access granted or denied)
6. SP then allows the user to connect (or not).

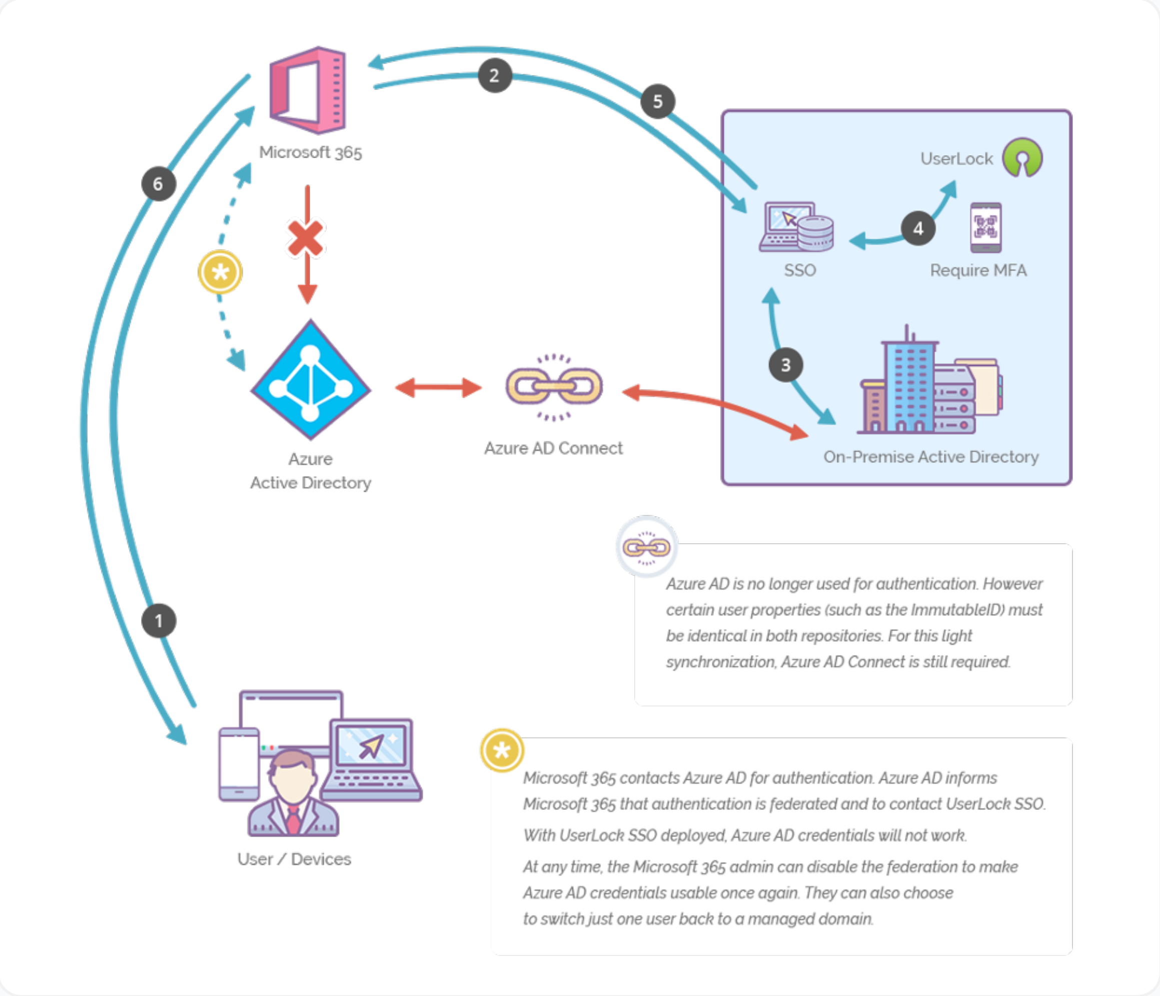
How UserLock single sign-on works

UserLock SSO for Micosoft 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.



Azure AD is no longer used for authentication. However certain user properties (such as the ImmutableID) must be identical in both repositories. For this light synchronization, Azure AD Connect is still required.

Microsoft 365 contacts Azure AD for authentication. Azure AD informs Microsoft 365 that authentication is federated and to contact UserLock SSO.

With UserLock SSO deployed, Azure AD credentials will not work.

At any time, the Microsoft 365 admin can disable the federation to make Azure AD credentials usable once again. They can also choose to switch just one user back to a managed domain.

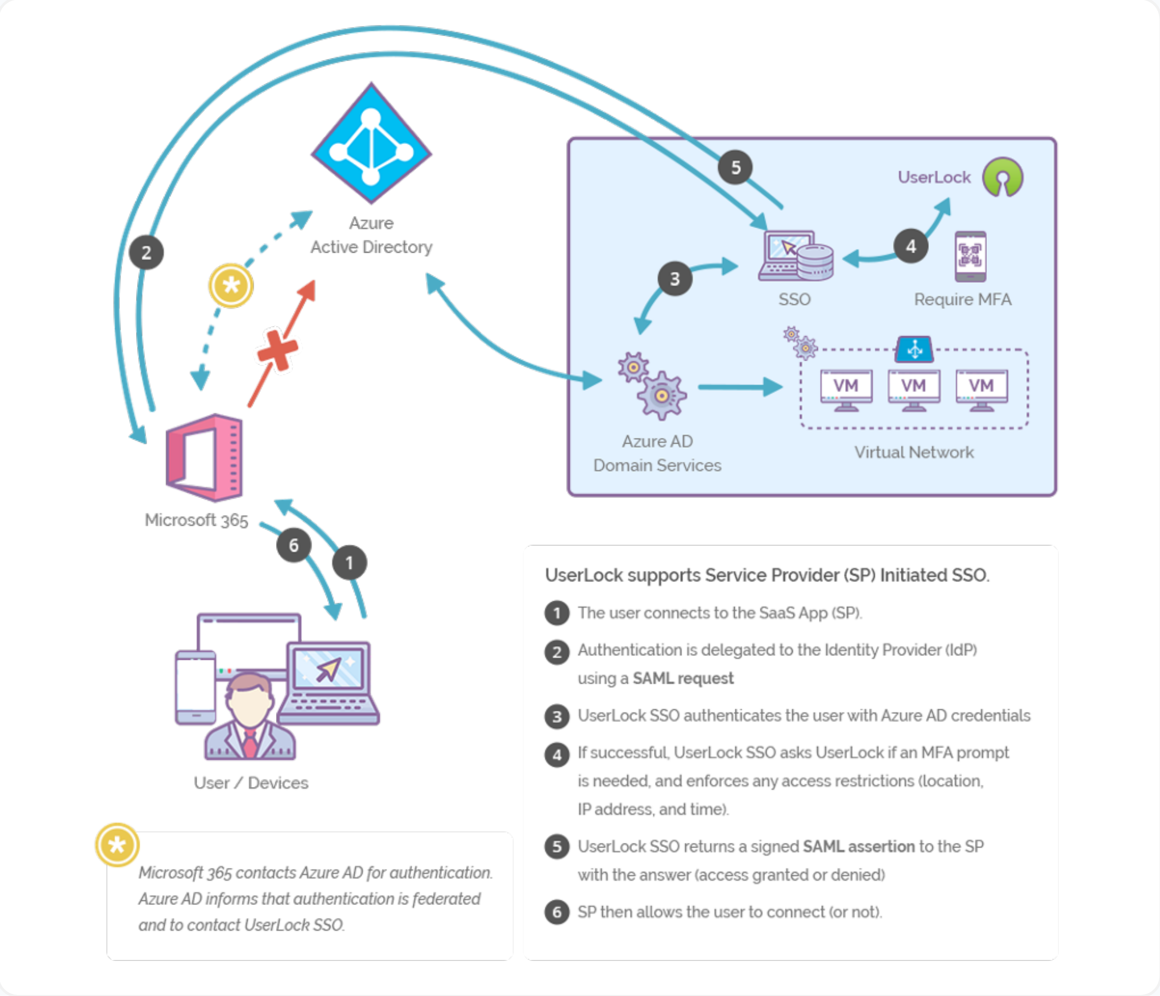
How UserLock single sign-on works

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.



Microsoft 365 contacts Azure AD for authentication. Azure AD informs that authentication is federated and to contact UserLock SSO.

UserLock supports Service Provider (SP) Initiated SSO.

1. The user connects to the SaaS App (SP).
2. Authentication is delegated to the Identity Provider (IdP) using a **SAML request**
3. UserLock SSO authenticates the user with Azure AD credentials
4. If successful, UserLock SSO asks UserLock if an MFA prompt is needed, and enforces any access restrictions (location, IP address, and time).
5. UserLock SSO returns a signed **SAML assertion** to the SP with the answer (access granted or denied)
6. SP then allows the user to connect (or not).

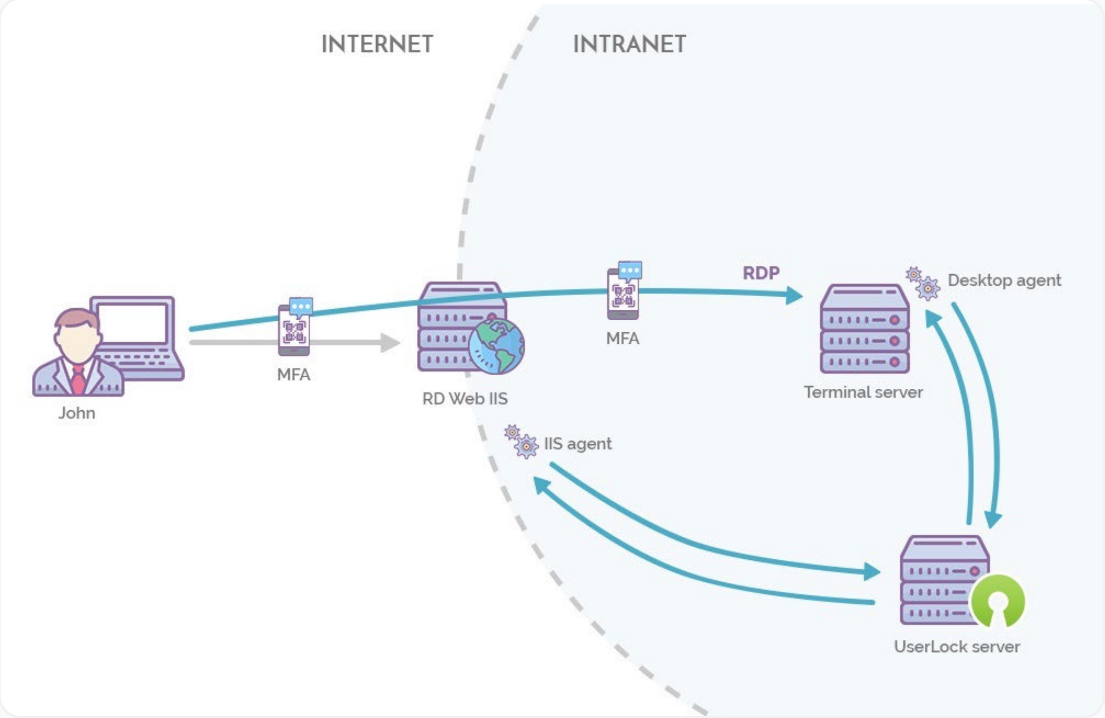
How UserLock secures RDP, RD Gateway, and RD Web

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.



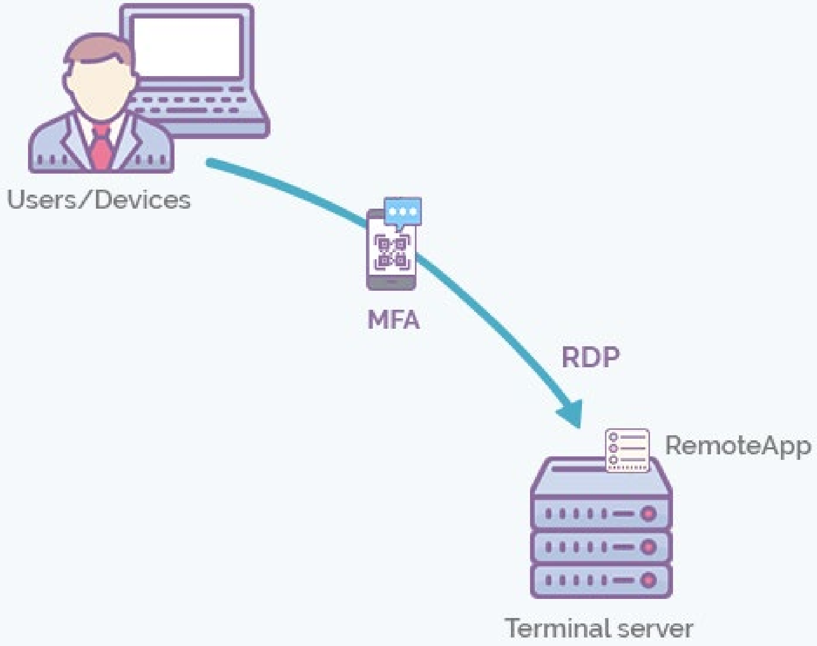
How UserLock secures RemoteApp access

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

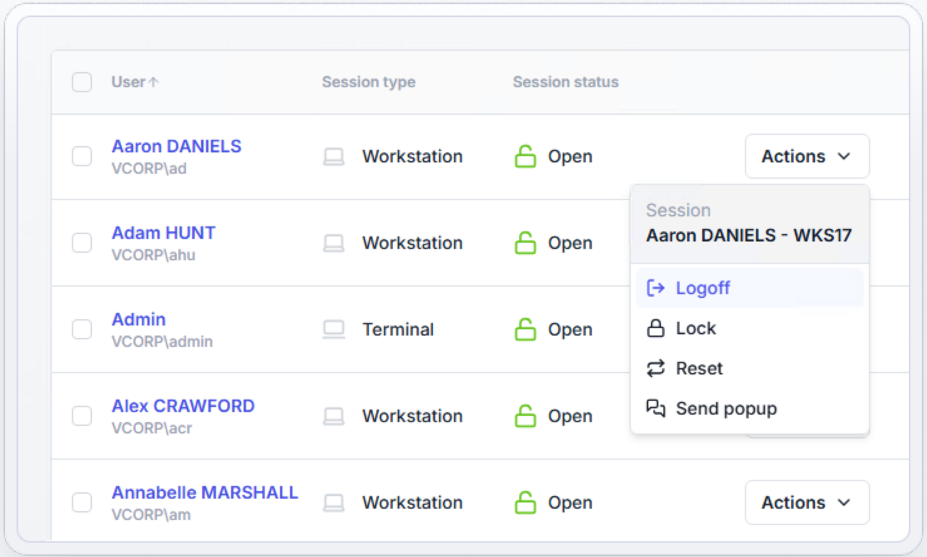
When you install UserLock, the MFA agent for OWA is installed on the existing IIS server. You can control when to prompt for MFA, based on: time of day, device location, and AD user, group, and OU.

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.



□	User ↑	Session type	Session status	
□	Aaron DANIELS VCORP\ad	Workstation	Open	Actions ⌄
□	Adam HUNT VCORP\ahu	Workstation	Open	
□	Admin VCORP\admin	Terminal	Open	
□	Alex CRAWFORD VCORP\acr	Workstation	Open	
□	Annabelle MARSHALL VCORP\am	Workstation	Open	Actions ⌄

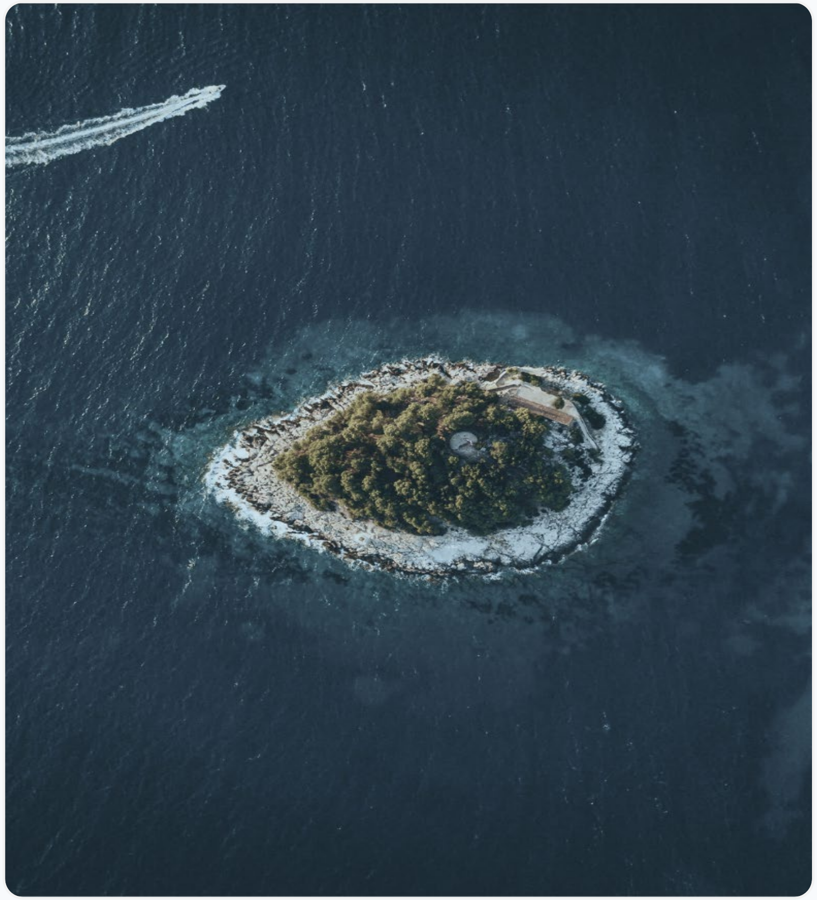
How UserLock secures air-gapped environments

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