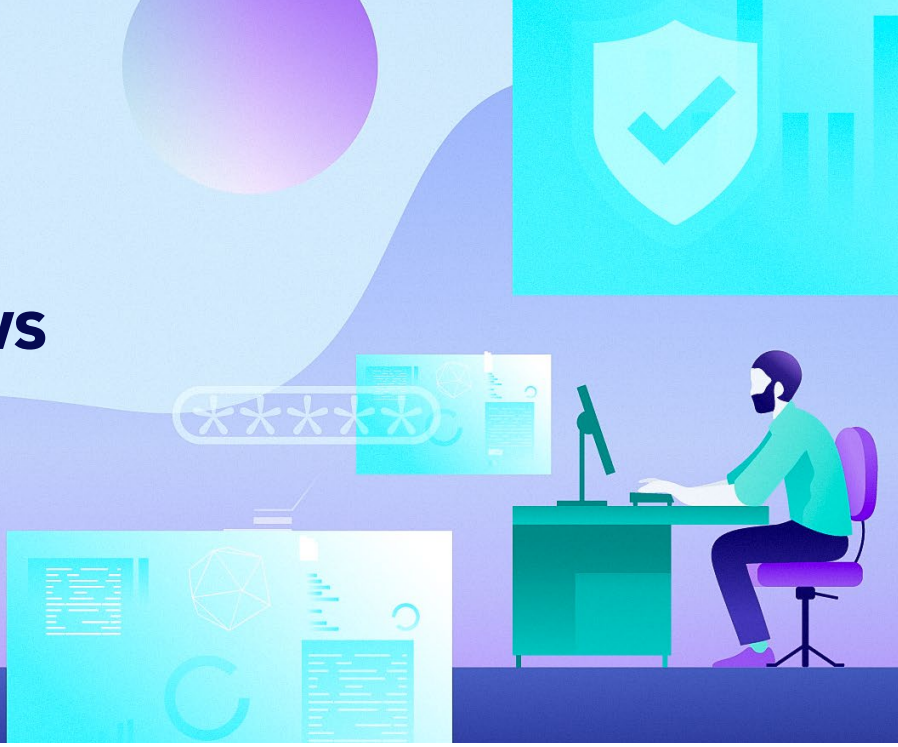
TeamViewer

TeamViewer Tensor

Microsoft Windows LAPS Integration

Privileged Access Management (PAM) for quick, structured, and elevated remote support



Introduction

TeamViewer Tensor was designed and purpose-built to offer robust enterprise security that doesn't compromise at any stage. Customers have leveraged the solution across many different industries and use cases to reduce configuration errors. And in highly secure environments, the margin for error becomes extremely slim.

As security has always been a core principle for TeamViewer, the integration with Microsoft Windows LAPS further solidifies our commitment to supporting customers who need to maintain their security posture with seamless privileged access management capabilities for their remote environment.

Customer challenges

Unsecure credential management

Often times, supporters need admin accounts to address issues during remote sessions. Gaining access to these credentials can be a cumbersome process and as a result can lead to poor password hygiene and mismanagement of credentials.

Complex privilege escalation

Employees will typically have limited accounts without the necessary permissions to change any critical settings, install, or modify any applications. This leads to a lengthy and complex process to request administrator-level rights and admin access to devices causing unnecessary friction.

Rising security threats

Effective password management is critical in highly secured environments, yet 54% of employees globally rely on memory to manage passwords and reuse credentials at work.[1] This behavior can be extremely risky, especially when elevated access is required.

Compliance difficulties

It has been recently reported that 34% of companies have lost business due to missing certifications.[2] Obtaining those certificates starts with meeting regulatory requirements and aligning on compliance. Having Privileged Access Management functionality to enable secure login transactions is now becoming a need rather than an option.

Multiple use cases

Just-in-time (JIT) privileges for IT Support

The ability to elevate privileges during a remote session is a common need amongst IT support professionals. In order to assist standard users with system-level changes and application installations, Windows LAPS integration with TeamViewer is essential for **resolving issues that require administrative access, such as configuring system settings or deploying software.** By enabling privilege escalation within the remote support environment, the supporter can efficiently address user needs without requiring physical access to the device or disrupting the user's workflow. This approach enhances responsiveness while maintaining security and control over administrative actions.

Elevated Remote Administration

Through the Windows LAPS integration with TeamViewer, **IT admins are able to securely perform tasks that require elevated privileges on remote machines.** This integration enables the administrator to install applications, modify system configurations, and carry out other administrative functions without compromising on security.
By leveraging LAPS, which provides unique and regularly rotated local admin passwords, the administrator ensures that remote access remains both secure and compliant with organizational policies.

Secure unattended access for IT maintenance

An IT admin may require TeamViewer to leverage LAPS -managed local administrator credentials to enable secure, unattended access to servers. **This setup facilitates remote maintenance and troubleshooting without needing end-user involvement, streamlining operational efficiency.** By automating credential management through LAPS, the administrator can ensure that **access remains tightly controlled**, reducing the risk of unauthorized entry while maintaining compliance with enterprise security protocol s. This approach is particularly valuable for managing large-scale environments where timely and secure remote interventions are critical.

Benefits at a glance

Secure access

Reduce user errors

Credential enforcement

Effective password management

Compliance alignment

Key benefits

Secure access

Secure and monitor access to critical systems and applications.

Reduce user errors

Scalable solution designed to minimize user errors.

Credential enforcement

Eliminate reliance on default admin accounts with known credentials.

Effective password management

Strengthen security through automatic password generation and rotation.

Compliance alignment

Support compliance efforts with robust access controls.

Feature highlights

- Enables **secure credential retrieval** and session management by connecting to Entra or Intune, injecting credentials into TeamViewer sessions, and triggering password rotation upon session close.
- Fetch and **inject credentials directly into login fields** during a TeamViewer session, with the option to copy them to the remote clipboard for seamless access.
- Provides an **audit trail** to determine who accessed or rotated a credential.
- **Privileged access is available from the new TeamViewer Tensor clients** on Windows.
- Supports Windows LAPS credentials retrieval **on Intune enrolled Windows 10 and Windows 11 remote devices.**

Contact TeamViewer to find out how Tensor's PAM capabilities can help secure your remote support operations.

Contact TeamViewer today

1. https://www.businesswire.com/news/home/20240424568925/en/Over-54-of-People-Globally-Rely-on-Memory-to-Manage-Passwords-and-Reuse-Credentials-at-Work
2. https://go.a-lign.com/Benchmark-Report-2024?_ga=2.256874313.375476182.1720816111-1932865074.1717625005

Stay connected