TeamViewer Tensor

DATASHEET

TeamViewer Tensor™ with Single Sign-On (SSO)

Enforce Your Security Policies With Simple and More Efficient SSO Authentication

TeamViewer Tensor integrates with your single sign-on (SSO) identity providers, using SAML 2.0 and SCIM protocols, including Okta, Azure AD, OneLogin, Centrify, G Suite, and Active Directory Federation Services (ADFS). This means you can add TeamViewer Tensor to your list of SSO business apps, eliminating the need for users to log in with separate credentials to start TeamViewer remote sessions.

Key Challenges

IT organizations implement remote access and support solutions so employees can work from anywhere, and IT can support their devices remotely. Along with convenience and efficiency, remote access comes with security demands that are particularly challenging for expanding mid-market and enterprise companies that need to:

- Stop unauthorized users and third parties from using company-licensed remote access to connect to their devices and network
- Keep track of who is using their enterprise remote connectivity platform
- Prevent employees and contractors from using personal TeamViewer accounts to access corporate devices
- Ensure the company security policies and guidelines are applied to every user account within the organization

As companies grow and provide remote access to more employees, they struggle with efficiently provisioning and deactivating TeamViewer account access in a timely manner, especially for departing employees.

These situations present different security risks, but they are also easy to solve.

How? By adding TeamViewer Tensor to your company's single sign-on provider.

Enhance Remote Access Security with Single Sign-On

TeamViewer Tensor with Single Sign-On gives IT more control over provisioning enterprise user accounts for TeamViewer Tensor remote access and support. By limiting access to users with corporate emails only, TeamViewer Tensor with SSO allows you to prevent unauthorized users from ever using your enterprise remote access platform. That means eliminating "rogue" or "shadow" use of personal or free TeamViewer accounts to access corporate devices.

Plus, when you add TeamViewer Tensor to your existing SSO identity service provider, you can deploy TeamViewer Tensor silently to authorized employees with corporate email accounts, without interrupting their productivity.

Simply put, *no one* can use TeamViewer Tensor without single sign-on permission.

- Centralize password control through your SSO identity service provider, so IT doesn't have to manage passwords, reducing password reset requests.
- Automatically apply corporate password policies and identity authentication rules to every authorized TeamViewer Tensor user.
- Efficiently offboard employees, without worrying about unauthorized backdoor access through TeamViewer.
- Improve the end user experience by allowing employees to log in to TeamViewer Tensor with the same SSO login credentials they're already using for your corporate applications — no separate TeamViewer Tensor login with another password to remember.

Feature Highlights

- **SAML 2.0 and SCIM Compatible**
  Integrates with popular identity providers like Okta, Azure, OneLogin, Active Directory Federation Services (ADFS), and any solution based on SAML 2.0 or SCIM protocols.
- **Automatic Policies**
  Apply existing corporate authorization and password policies to TeamViewer Tensor users through SSO.
- **Multifactor Authentication**
  Leverage multifactor authentication for added security.
- **Automated Status Changes**
  Automatically update changes to active accounts and deactivate user accounts, ensuring only approved corporate email addresses access TeamViewer Tensor.
- **Remote Credential Setup**
  Instantly set and reset account credentials from anywhere.

Key Benefits

Improve Usability

With *one* set of SSO login credentials to access all your apps, your employees won't have to log in separately each time to start TeamViewer Tensor sessions.

Increase IT Security

Instantly increase security by granting single sign-on access to TeamViewer Tensor for corporate emails only, preventing unauthorized users from logging in with external emails.

Boost IT Efficiency

Centrally provision and deactivate TeamViewer Tensor account access through SSO.

Ensure Corporate Security Compliance

Automatically apply company-defined password policies and authentication to all users, passed on by your identity provider to ensure corporate security compliance.

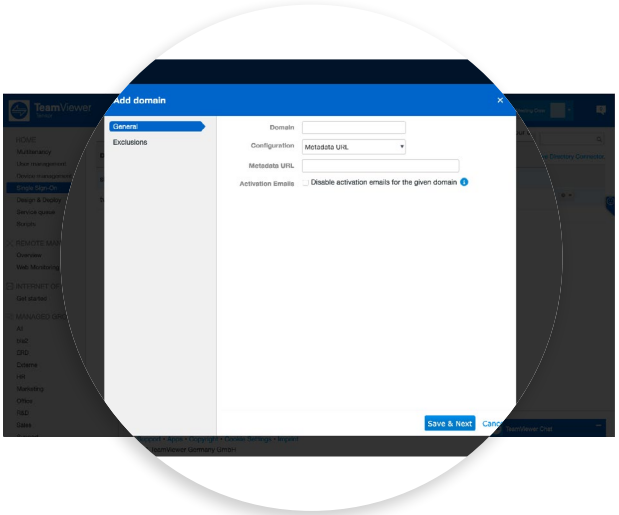

Figure 1: Through the TeamViewer Management Console, connect to your single sign-on provider service by adding your domain and metadata URL.

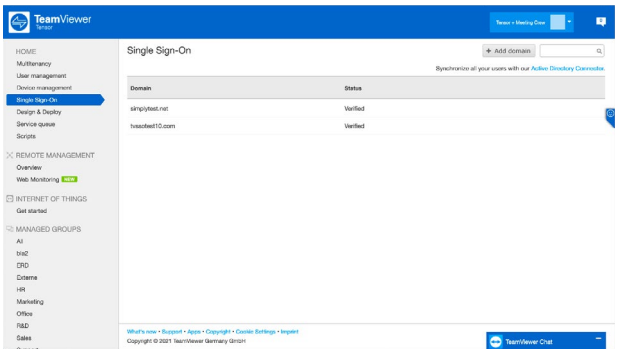

Figure 2: Overview of your verified domains connected with single sign-on.

About TeamViewer

As a leading global remote connectivity platform, TeamViewer empowers users to connect anyone, anything, anywhere, anytime. The company offers secure remote access, support, control, and collaboration capabilities for online endpoints of any kind and supports businesses of all sizes to tap into their full digital potential. TeamViewer has been activated on approximately 2.5 billion devices, up to 45 million devices are online at the same time.

Founded in 2005 in Göppingen, Germany, TeamViewer is a publicly held company listed on the Frankfurt Stock Exchange, employing about 1,350 people in offices across Europe, the US, and Asia Pacific.

Stay Connected

www.teamviewer.com