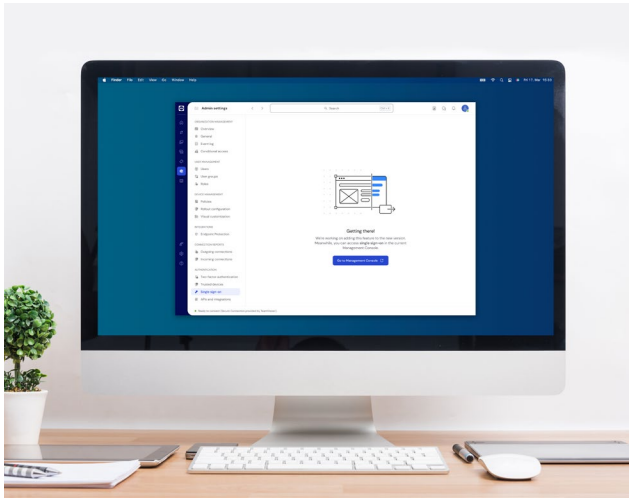
TeamViewer

# TeamViewer Tensor
# Single Sign-On (SSO)

**Enforce security policies and boost efficiency with Single Sign-On (SSO).** TeamViewer Tensor integrates with your single sign-on (SSO) with leading identity providers, using SAML 2.0 and SCIM protocols such as Okta, Azure AD, OneLogin, Centrify, G Suite, and Active Directory Federation Services (ADFS). Save time and effort for users to easily log in and start TeamViewer remote sessions to support employees, partners and stakeholders in your organization.

**Overview**
Remote connectivity can enable IT organizations to empower employees to work from anywhere and provide real time remote support for technical issues that can sometimes happen in a regular working day. However, remote connectivity comes with security requirements that can particularly challenging for mid-market and enterprise companies that need to:

- Prevent unauthorized users and third parties from using company-licensed remote access to connect to their devices and network
- Have greater visibility on 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 connectivity to more employees, they struggle with efficiently provisioning and deactivating TeamViewer account access in a timely manner, especially for employees that are no longer with the organization.

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

# Enhance remote access security with **Single Sign-On (SSO)**

TeamViewer Tensor with SSO 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 using your enterprise remote connectivity 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.

TeamViewer Tensor with SSO allows you to prevent unauthorized users from using your enterprise remote connectivity platform.

# 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

# 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.

TeamViewer

## About TeamViewer

As a leading global technology company, TeamViewer offers a secure remote connectivity platform to access, control, manage, monitor, and support any device — across platforms — from anywhere. With more than 600,000 customers, TeamViewer is free for private, non-commercial use and has been installed on more than 2.5 billion devices. TeamViewer continuously innovates in the fields of Remote Connectivity, Augmented Reality, Internet of Things, and Digital Customer Engagement, enabling companies from all industries to digitally transform their business-critical processes through seamless connectivity.

Founded in 2005, and headquartered in Göppingen, Germany, TeamViewer is a publicly held company with approximately 1,400 global employees. TeamViewer AG (TMV) is listed at Frankfurt Stock Exchange and belongs to the MDAX.


www.teamviewer.com/support

**TeamViewer Germany GmbH**
Bahnhofsplatz 2 73033 Göppingen Germany
+49 (0) 7161 60692 50

**TeamViewer US Inc.**
5741 Rio Vista Dr Clearwater, FL 33760 USA
+1 800 638 0253 (Toll-Free)


**Want to know more?**

Scan the QR Code to discover more about Teamviewer Tensor or contact us

+49 7161 60692 50

## Stay Connected

www.teamviewer.com