



TeamViewer
Tensor

DATASHEET
For Resellers

Secure Enterprise Remote Access and Support with TeamViewer Tensor

TeamViewer Tensor™ is a highly scalable remote connectivity cloud platform with enterprise-grade security features, enabling organizations to remotely access, support, and control any device or machine quickly and easily from anywhere, anytime.

With companies pivoting quickly to remote and hybrid-remote workplaces, accelerated by the global COVID-19 pandemic, IT organizations are struggling with new security concerns and complex challenges to support work-from-home environments:

- Remote workers aren't always able to connect to their corporate VPN
- Implementing additional VPN infrastructure takes several weeks to months
- The need for digital collaboration has given rise to tools with uncertain or even nonexistent security standards
- The increase in remote work has accelerated the success rate of phishing email scams

TeamViewer Tensor

Powered by the world's largest remote connectivity infrastructure — spanning 200 countries and connecting more than 2.5 billion devices — TeamViewer Tensor scales linearly to meet enterprise requirements, providing fast, reliable connectivity and real-time support tools in a secure, instantly deployable SaaS environment.

Maximize IT and Employee Productivity with Easy-to-Use Remote Access and Support

TeamViewer Tensor enables remote experts to support any computer or mobile device — from anywhere, at any time, on any platform — and fix technical issues to minimize downtime, while improving IT and workforce productivity.

When working from home or working on-the-go, your enterprise IT teams and employees can stay productive from anywhere with secure remote access to computers, mobile devices, servers, machines, or operational technology (OT). With TeamViewer Tensor remote access, your desktop files and corporate applications are always just a few clicks away.



Enable your organization to work securely from anywhere to keep your business running efficiently — all without VPN.

- ✓ Offer remote work flexibility by enabling your workforce to remotely connect to corporate computers and mobile devices across platforms, from anywhere, anytime.
- ✓ Remotely manage, monitor, and control industrial equipment and machines to improve operational efficiency, reduce issue resolution time, and maximize uptime.
- ✓ Maintain and manage enterprise servers and Android-based point-of-sale (POS) systems, troubleshooting problems from anywhere in real time to minimize unplanned downtime.

Secure Remote Connectivity



1,400+ Enterprise Customers



2.5+ Billion Installations



600K+ Subscribers

TeamViewer Tensor Security Features



At TeamViewer, security always comes first. We believe security is a combination of state-of-the-art technology, best practices, and discipline.



The TeamViewer ID

The TeamViewer ID is unique to your device, which is generated automatically and checked before each session.



Industry-Grade Security Standards

Our data centers meet ISO 27001 industrial security standards.



Protection from Brute-Force Attacks

With TeamViewer, the time between failed login attempts is increased exponentially and is reset only when the correct password is entered. It also protects remote access devices and connection partners from other attacks.



Two-Factor Authentication

Login takes place using a new unique code, which is generated each time by an algorithm and supplied from a mobile device.



Secure Remote Protocol (SRP)

TeamViewer uses the SRP protocol for authentication and password encryption. So, the password is never sent over the internet, even encrypted, and is therefore optimally protected from outside access. Passwords also receive backend encryption.



Encryption

All interactions through TeamViewer, including file transfers, VPN, chat, etc., are protected by 256-bit end-to-end session encryption with a 4096-bit RSA public/private key exchange.

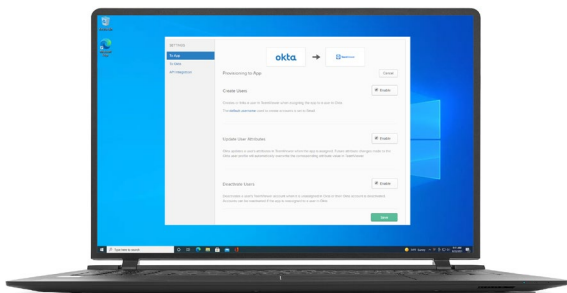


Dynamic TeamViewer Password

Users can create a policy that auto-generates a new dynamic session password after each TeamViewer service restart. But there is also an optional setting which allows a password to be set dynamically after each session. This password is alphanumeric as standard, and comprises six characters, so there are over 2.1 billion possible combinations.

Enterprise Security Features

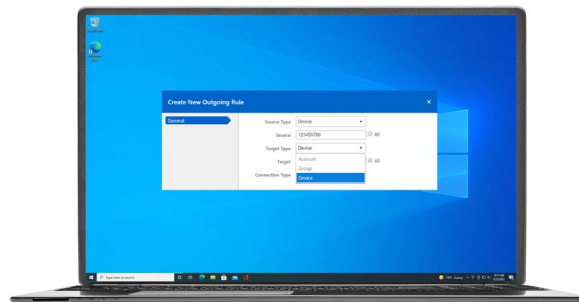
With TeamViewer Tensor, organizations can leverage industry-leading remote connectivity with enterprise-grade security features and capabilities — all designed to ensure your data, connections, and employees remain secure.



Single Sign-On (SSO)

With Single Sign-On, IT has more control over provisioning and deactivating enterprise user accounts for TeamViewer Tensor. 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.

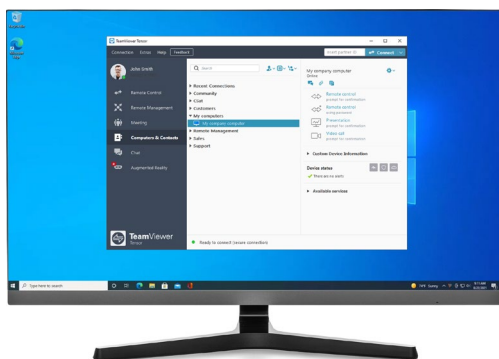
- ✓ Centralize password control through your SSO identity service provider, so IT doesn't have to manage passwords, reducing password reset requests.
- ✓ Automatically apply corporate password policies and identity authentication rules to every authorized TeamViewer Tensor user.
- ✓ Enable employees to log in to TeamViewer Tensor with their corporate SSO login credentials.



Conditional Access

With TeamViewer Tensor Conditional Access, enterprise IT and security managers can maintain company-wide oversight of TeamViewer access and usage from a single location.

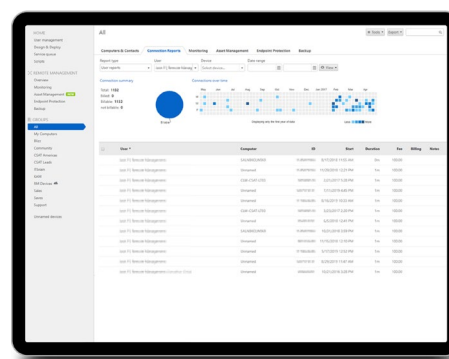
- ✓ Centralized rules management within the Management Console.
- ✓ Assign remote control permissions.
- ✓ Manage file transfer permissions through policies.
- ✓ Configure rules at the account, group, or device level, with support for Active Directory Groups (Active Directory and Azure Active Directory).
- ✓ TeamViewer manages and maintains dedicated infrastructure.
- ✓ Supports Windows, macOS, iOS, and Android devices.
- ✓ Manage access for TeamViewer Assist AR.



Mass Deployment

Network administrators with approved security access can install and update TeamViewer Tensor silently on all your corporate computers and mobile devices.

- ✓ Silently roll out deployment to attended and unattended devices, without disrupting end users.
- ✓ Script complex multistep tasks to eliminate manual processes.
- ✓ Pass on existing account assignment from systems that leverage MSI packages.
- ✓ Mass deploy to tens of thousands of devices in hours, not weeks.



Comprehensive Logging and Reporting

Built-in reporting log captures all remote session activities and management console actions: who did what, when, and for how long for every incoming and outgoing connection. Designated IT admins can only view these audit logs with appropriate user permissions.

- ✓ Decide if activity log for remote sessions and management console is needed or not, with Opt In/Opt Out feature.
- ✓ Assign specific user permissions authorizing access to view reports.
- ✓ Maintain accountability and provide precise billing for services.
- ✓ Track customer satisfaction with session comments and customer feedback forms to improve services.
- ✓ Cut costs by eliminating the need for third-party logging tools.

Certifications and Compliance



ISO 9001:2015

ISO 9001:2015 is the globally recognized standard that specifies requirements for a quality management system (QMS). Organizations use the standard to demonstrate their ability to consistently provide products and services that meet customer and regulatory requirements.

With the ISO 9001:2015 certification, TeamViewer has demonstrated dedication to total quality management, customer focus, and a continuous improvement of processes to increase efficiencies and enhance the quality of products and services offered.



The Trusted Information Security Assessment Exchange assesses the information security of enterprises and allows recognition of assessment results among the participants, who conduct business in the automotive supply chain.



As an additional security measure, we secure all our program files using DigiCert code signing technology, so the actual publisher of the software is always readily identifiable. If the software has been changed afterwards, the digital signature automatically becomes invalid.

HIPAA, HITECH, and SOC2



TeamViewer provides remote access, remote support, and online collaboration capabilities with the level of security and privacy necessary for organizations to remain HIPAA compliant.



HIPAA, HITECH, and SOC2 Certified TeamViewer received HIPAA, HITECH, and SOC2 certification from A-LIGN, a U.S. nationwide security and compliance provider. While HIPAA and HITECH are crucial for health care organizations to ensure the confidentiality and security of sensitive data and protected health information (PHI), SOC2 is an essential reporting framework for service provider organizations to establish a means to report on nonfinancial internal controls, so that their clients get a better understanding of the enforcement of the five Trusted Service Principles (TSP).

General Data Protection Regulation (GDPR)

On May 25, 2018, the EU [General Data Protection Regulation \(GDPR\)](#) came into force, reflecting the importance of data protection in our increasingly digital world. TeamViewer is a global organization and for us, it is important that we handle the personal information of our customers and our own people under GDPR.

To learn more about TeamViewer's data privacy commitment and GDPR preparation, visit the [TeamViewer and GDPR](#) page in our Knowledge Base.

For more information about TeamViewer security, explore the [TeamViewer Security Handbook](#).

California Consumer Protection Act (CCPA)

On June 28, 2018, the [California Consumer Protection Act of 2018 \(CCPA\)](#) was signed into law and took effect on January 1, 2020. TeamViewer is committed to CCPA compliance and data privacy. To learn more, please visit the [TeamViewer and CCPA](#) page in our Knowledge Base.

Questions?

Connect with us today to discuss a tailored solution that fits your needs.

✉ AmericasPartners@teamviewer.com

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.

Stay Connected



www.teamviewer.com