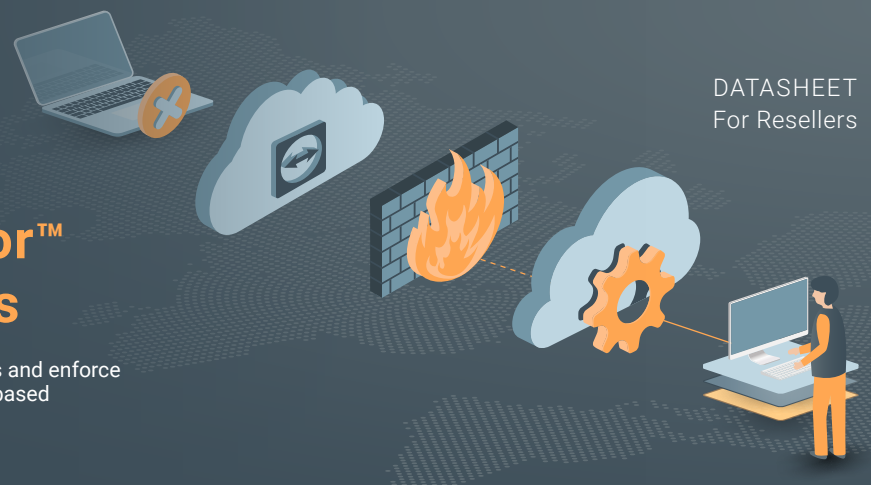
TeamViewer Tensor

DATASHEET
For Resellers



TeamViewer Tensor™ Conditional Access

Prevent unauthorized remote access connections and enforce corporate security policies with a dedicated rule-based conditional access router.

Key Challenges

As remote access and remote support have become business-critical for organizations, IT departments struggle with a lack of total visibility and control over remote connections and user permissions.

Organizations managing remote access at enterprise scale need full control of permissions at the user, device, and group levels to maintain corporate security compliance and eliminate unauthorized activities. Moreover, IT administrators need to control permissions for sensitive features, like scripts and file transfers, to mitigate risks and keep their network perimeter secure.

Plus, they need to block unauthorized remote access from personal or free TeamViewer accounts, while provisioning remote access for third-party vendors, temporary employees, and contractors to get their work done during a specified period of time.

So, how can you control remote access to and from your network and devices? And, how do you ensure that only the right people have the right access to the right systems, with the right features, at the right time?

That's where TeamViewer Tensor Conditional Access comes in to help enterprises gain total control over all incoming and outgoing connections, while enabling IT administrators to define which users can access which devices and features, when and for how long.

TeamViewer Tensor: Conditional Access

TeamViewer Tensor Conditional Access enables enterprises to control all incoming and outgoing TeamViewer connections at the user, group, and device levels by using a dedicated conditional access router with a rule-based engine.

- Define and enforce user and device access rights for remote access sessions.
- Provide added security to remote connections by preventing unauthorized use of sensitive features, like Scripts and File Transfer.
- Provision temporary remote access to specific devices with restricted functionality and expiring permissions for third-party vendors, contractors, or temporary employees.

Technical Requirements

- Activated TeamViewer Tensor Pro or TeamViewer Tensor Unlimited license; or TeamViewer Tensor with Conditional Access AddOn
- TeamViewer Client version 15.5 or higher
- TeamViewer company profile created in the Management Console
- DNS/IP address of dedicated conditional access router

Feature Highlights

Conditional Access Router

Protect network perimeter access by controlling all connections with a dedicated rule-based conditional access router or "gatekeeper," provisioned and maintained in your own private cloud by TeamViewer.

Granular Permission Control

Define remote access rules and restrict available features at the user, group, and device levels for centralized management and granular control over all incoming and outgoing connections.

Expiring Access Rules

Create and schedule customized time-based permissions with expiring access rules for users outside your network — such as third-party vendors, contractors, and temporary employees — defining who has access to which devices and features within a specified date and time frame.

Privileged Access Management

Reduce risks by assigning privileged access rules for specified users, with different permissions to sensitive features — such as scripts or file-sharing — than standard users when connecting to the same devices or network systems.

Block Meetings

Decide if your company needs access to TeamViewer Meeting for videoconferences, VoIP calls, and instant chats, or block meeting capabilities for all users according to your requirements.

How TeamViewer Tensor Remote Connections Work

Without Conditional Access

VS.

With Conditional Access

Employee Remote Support

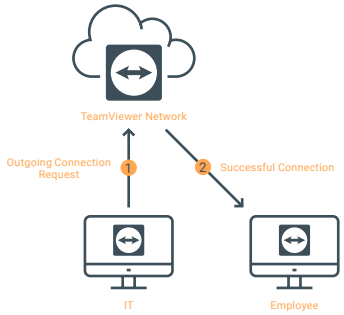


Figure 1a: Authorized remote support for employees — IT administrator successfully connects to employee's device within company network.

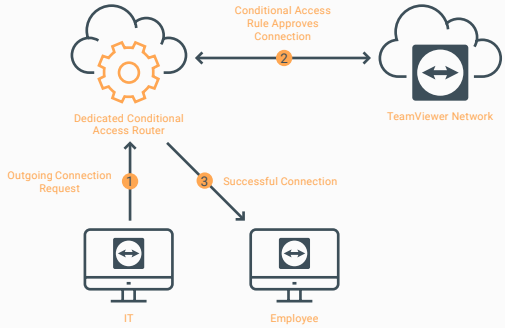


Figure 1b: Authorized remote support for employees — IT administrator connects to the conditional access router that approves access to employee's device within company network.

Customer Support

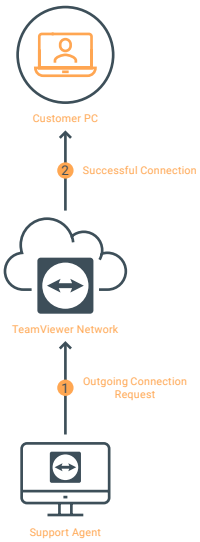


Figure 2a: Authorized customer support connection — Support agent successfully connects to customer's device outside the company network.

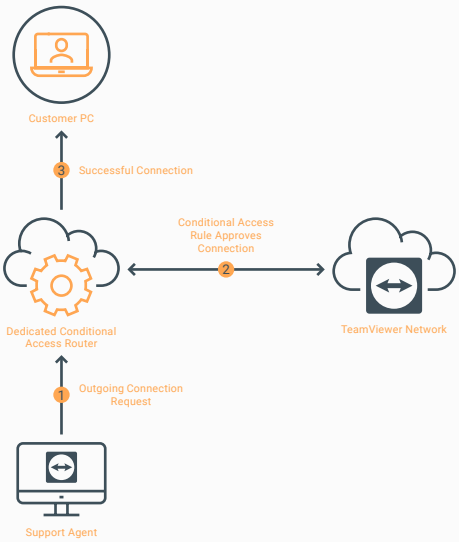


Figure 2b: Authorized customer support connection — Support agent successfully connects to the conditional access router that approves access to customer's device outside the company network.

Unauthorized Remote Connection

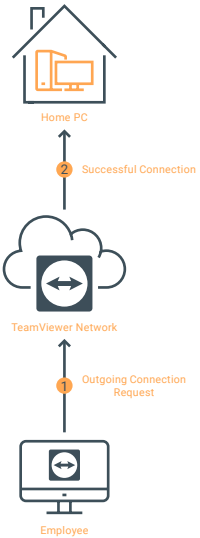


Figure 3a: Unauthorized connection from company network to personal device — Employee successfully connects from work to personal device at home.

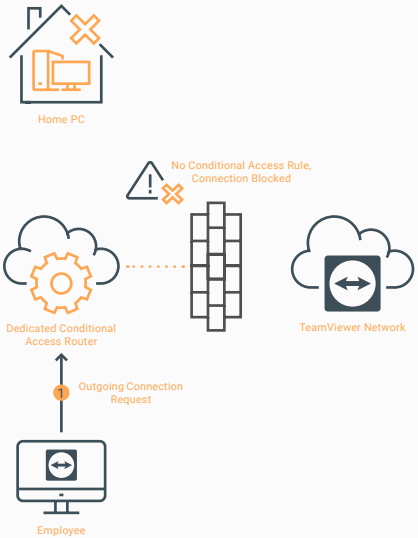


Figure 3b: Unauthorized connection from company network to personal device — Employee fails to connect from work to personal device at home.

How It Works

TeamViewer provisions and maintains your Conditional Access router in a secure, private cloud. The Conditional Access router is powered by a rule-based engine, which acts like a gatekeeper authorizing and blocking remote connections.

Once the rule-based engine has been configured, IT administrators can activate Conditional Access to authorize access for users, groups, and devices. If rules are inactive — such as during initial setup or maintenance — Conditional Access is deactivated by default, blocking all TeamViewer connection attempts.

IT administrators can centrally manage, define, filter, and edit Conditional Access rules in the TeamViewer Tensor Management Console for users, groups, and authorized computers* or devices with customizable permissions for specific features and functions:

- ✓ Select different options for different users and rules for more secure permission handling
- ✓ Set required conditions to authorize access rights for users, groups, or network devices
- ✓ Define and schedule remote access rules with customizable expiration dates and times, increasing security for third-party vendors, partners, and contractors

**Supported platforms: Windows and macOS*

Without Conditional Access

Without Conditional Access, IT administrators can only **block incoming** connections to devices in your network, so users can connect to any device, whether it's approved by IT or not.

- ✓ Approved, connection possible: Employee devices within the network (*Figure 1a*)
- ✓ Approved, connection possible: Customer devices outside the network (*Figure 2a*)
- ✓ Unapproved, connection possible: Personal servers and devices at home (*Figure 3a*)

All encrypted data goes through the TeamViewer Network.

With Conditional Access

With Conditional Access, IT administrators can **block incoming and outgoing** connections, so users can only connect to devices based on predefined rules.

- ✓ Approved by rules, connection possible: Employee devices within the network (*Figure 2a*)
- ✓ Approved by rules, connection possible: Customer devices outside the network (*Figure 2b*)
- ✕ Unapproved, no rules, connection blocked: Personal servers and devices at home (*Figure 3b*)

All encrypted data goes through the Conditional Access router *only*.

Key Benefits

Increase IT Security

Keep your network perimeter protected from unauthorized remote access attempts, including all incoming and outgoing connection requests from free or personal TeamViewer account users.

Enhance IT Control

Get full control over how all users connect to devices, including assigning remote access permissions for third-party vendors, contractors, and temporary employees based on which devices and features they need to access within a defined period of time.

Mitigate Risks

Leverage privileged access management and expiring access rules to stay compliant with corporate security policies and mitigate risks of unauthorized remote access activities.

Boost IT Efficiency

Boost productivity and operational efficiencies with centralized management and control of all incoming and outgoing connections, as well as user access rights.

Improve Usability

Enable employees, consultants, and vendors to work remotely with easy-to-use features, enabling secure access to authorized network systems, computers, and devices — without VPN provisioning.

Reduce Costs

Reduce the total cost of ownership with a cloud infrastructure, managed and maintained by TeamViewer.

Questions?

Connect with us to request a free consultation and demo of TeamViewer Tensor.

channelpartner@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