TeamViewer

TeamViewer Tensor Conditional Access

Introduction

Conditional Access empowers company administrators to maintain robust control over inbound and outbound connections, critical for supporting various stakeholders within an organization. It acts as a potent safeguard against unauthorized remote access connections and enforces comprehensive security policies through an advanced rule-based Conditional Access router.

Customer **challenges**

Security concerns
Ensuring that remote access is secure and only granted to authorized users is a top priority. Unauthorized access can lead to data and security breaches in the organization.

Compliance requirements
Many industries have stringent regulatory compliance standards that must be met, such as HIPAA or GDPR. Ensuring compliance with these standards when providing remote access is crucial.

Resource optimization
Businesses need to optimize resource allocation, ensuring that remote access is granted only when necessary, to maximize productivity and minimize security risks.

Geographical restrictions
Some organizations may require remote access to be granted only from specific geographical locations to prevent unauthorized access from locations that are deemed risky.

Use cases

Control permissions for sensitive features, like scripts and file Transfers

Block unauthorized connections from personal or free TeamViewer accounts

Provisioning remote access for third party vendors, temporary employees, and Contractors

Ensuring only the right people have the right access to the right systems, at the right time

Key benefits **in a nutshell**

Increase IT security

Granular control

Mitigate risks

Boost efficiency

Greater flexibility

Key benefits

Utilizing a Conditional Access rule-based engine and a Conditional Access router, enterprise IT and security managers gain centralized control over TeamViewer access and usage across their organization.

Enhanced security
Benefit from an elevated security standard, as our system automatically terminates each connection after the pre-approved time period.

Streamlined control
Manage all connections through a dedicated conditional access router hosted and maintained by TeamViewer.

Rule customization
Admins can easily select and manage access rules with reuse options.

Access expiry
Set expiry dates for Conditional Access rules, restricting third-party and temporary worker access.

Centralized management
Efficiently manage rules within the Management Console.

Granular permissions
Assign permissions for remote sessions, file transfers, and meetings.

Flexible configuration
Configure rules at the account, group, or device level.

Beyond on-premises solutions
Enjoy the flexibility and simplicity of a cloud-based approach, offering scalability and accessibility beyond on-premises solutions.

Feature **highlights**

Conditional Access router
Enhance network perimeter security by managing all connections through a dedicated, rule-based Conditional Access router, provisioned and maintained within your private cloud by TeamViewer.

Precise permission management
Exercise granular control by establishing remote access rules and limiting available features at the user, group, and device levels. This centralized approach ensures precise management of all incoming and outgoing connections.

Time-based access rules
Create and schedule customized, time-based permissions using expiring access rules. These rules are especially useful for external parties like third-party vendors, contractors, and temporary employees, allowing you to define access to specific devices and features within specified date and time frames.

Privileged access management
Mitigate risks by assigning privileged access rules to designated users. This provides varying permissions, such as for scripts or file sharing, compared to standard users when connecting to the same devices or network systems, enhancing security for critical features.

How TeamViewer Tensor **remote connections work**

Without Conditional Access	With Conditional Access

Employee remote support

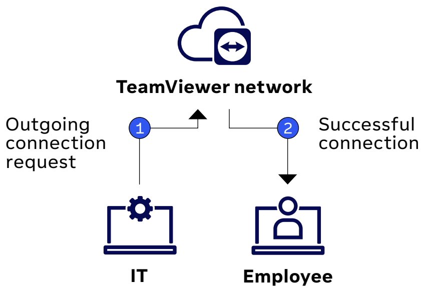


Figure 1a

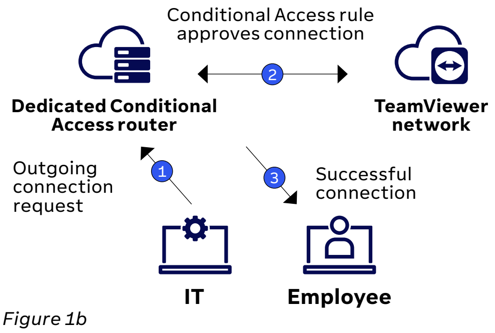

Conditional Access rule approves connection
2
Dedicated Conditional Access router
TeamViewer network
Outgoing connection request
1
3
Successful connection
IT
Employee

Figure 1b

Customer support

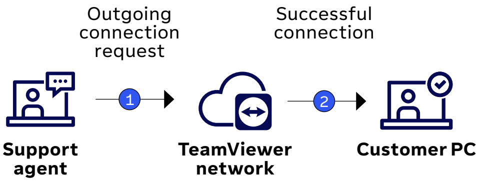


Figure 2a

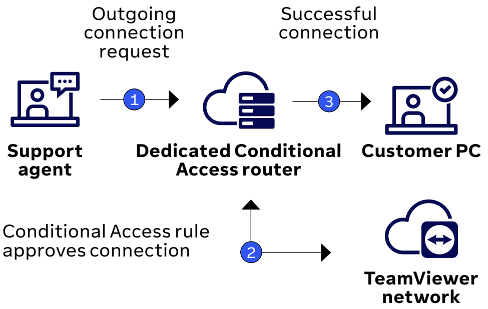

Outgoing connection request
Successful connection
1
3
Support agent
Dedicated Conditional Access router
Customer PC
Conditional Access rule approves connection
2
TeamViewer network

Figure 2b

Unauthorized remote connection

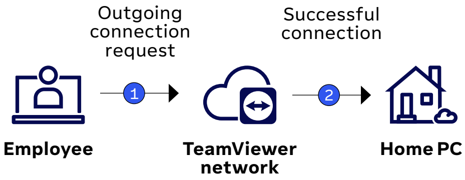


Figure 3a

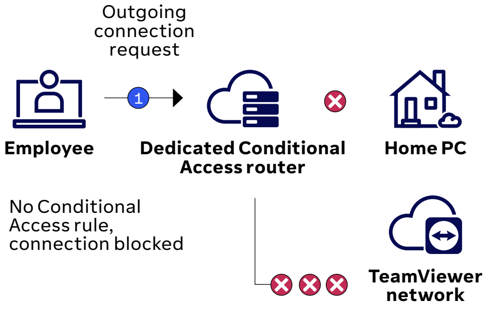
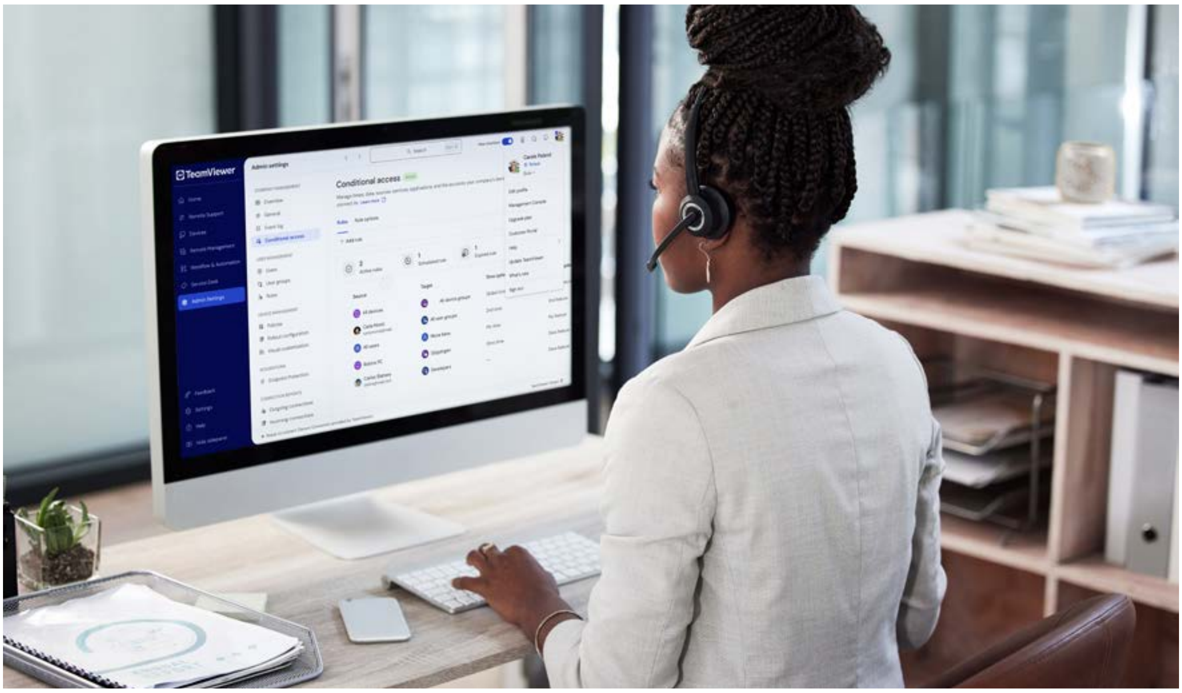

Outgoing connection request
1
Employee
Dedicated Conditional Access router
Home PC
No Conditional Access rule, connection blocked
TeamViewer network

Figure 3b

Figure 1a: Authorized remote support for employees — IT administrator successfully connects to employee's device within company network.
Figure 2a: Authorized customer support connection — Support agent successfully connects to customer's device outside the company network.
Figure 3a: Unauthorized connection from company network to personal device — Employee successfully connects from work to personal device at home.

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.
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.
Figure 3b: Unauthorized connection from company network to personaldevice — 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 specific users, groups, and devices.

IT administrators can centrally manage, define, filter, and edit Conditional Access rules in TeamViewer Tensor. If rules are inactive — such as during initial setup or maintenance — Conditional Access is deactivated by default, blocking all TeamViewer connection attempts.

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

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