TeamViewer

TeamViewer Tensor Conditional Access

Conditional Access enables company administrators to better control all incoming and outgoing connections that are needed to provide support to various stakeholders within an organization.

Conditional Access prevents unauthorized remote Access connection and enforces company-wide security policies with an advanced rule-based Conditional Access router.

Overview
Remote connectivity is business-critical for organizations that understand the increasing benefits of ensuring their employees, partners and various stakeholders are supported at all times.

Employees working - remotely, on the move or in a traditional office - can stay productive at all times if they can request support and are supported in a secure manner. However, IT departments often struggle with a lack of total visibility and control over remote support connections that happen and the increasing complexity of managing those growing connections within an organization can sometimes be a challenge.

Organizations managing remote connectivity access at scale need full, granular control of permissions at the user, device, and group levels. Conditional Access ensures they can do this and more while maintaining corporate security compliance and eliminating unauthorized access.

Conditional Access **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

TeamViewer **Tensor**

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

- **Enabling time-based option** for unattended access by internal IT or 3rd party support provider outside of business hours.
- **Defining and enforcing user** and device access rights for remote Access sessions.
- **Providing added security** to remote connections by preventing unauthorized use of sensitive features, like Scripts and File Transfer.
- **Provisioning temporary remote access** to specific devices with restricted functionality and
- **Expiring permissions for third-party vendors**, contractors, or temporary employees.

Feature **highlights**

Conditional Access router
Protect network perimeter access by controlling all connections with a dedicated rule-based Conditional Access router provisioned and maintained in your own private cloud by TeamViewer.

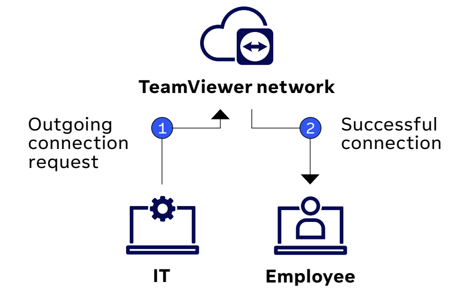
Granular permission control
Define remote access rules and restrict available features at the user, group, and device levels for centralized management and granular control over all incoming and outgoing connections.

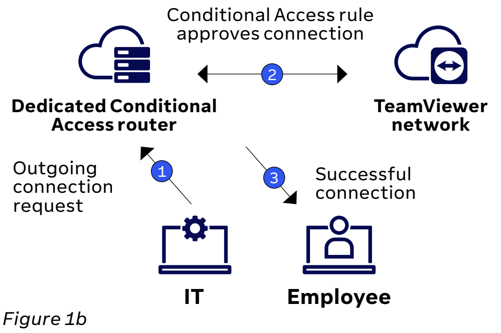
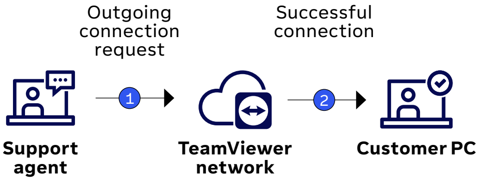
Expiring access rules
Create and schedule customized time-based permissions with expiring access rules for users outside your network — such as third-party vendors, contractors, and temporary employees — defining who has access to which devices and features within a specified date and time frame.

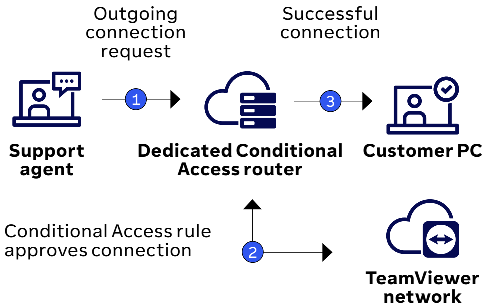
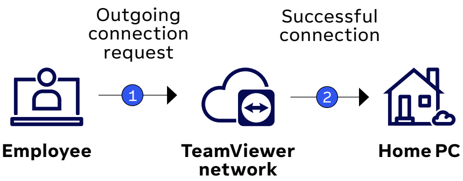
Privileged access management
Reduce risks by assigning privileged access rules for specified users, with different permissions to sensitive features — such as scripts or file-sharing — than standard users when connecting to the same devices or network systems.

TeamViewer Tensor enables enterprises to control all incoming and outgoing remote support connections.

How TeamViewer Tensor **remote connections work**

<table>
<tr><th>Without Conditional Access</th><th>With Conditional Access</th></tr>
<tr><td colspan="2"><b>Employee remote support</b></td></tr>
<tr><td>

<i>Figure 1a</i></td><td>
Conditional Access rule approves connection
Dedicated Conditional Access router
2
TeamViewer network
Outgoing connection request
1
3
Successful connection
IT
Employee
<i>Figure 1b</i></td></tr>
<tr><td colspan="2"><b>Customer support</b></td></tr>
<tr><td>

<i>Figure 2a</i></td><td>
Outgoing connection request
Successful connection
Support agent
1
Dedicated Conditional Access router
3
Customer PC
Conditional Access rule approves connection
2
TeamViewer network
<i>Figure 2b</i></td></tr>
<tr><td colspan="2"><b>Unauthorized remote connection</b></td></tr>
<tr><td>

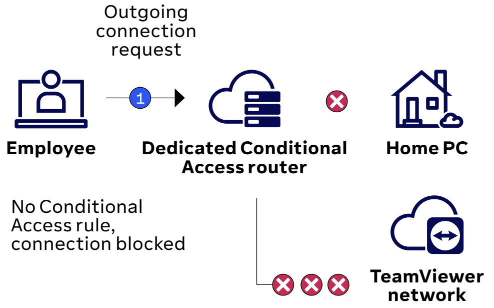
<i>Figure 3a</i></td><td>
Outgoing connection request
Employee
1
Dedicated Conditional Access router
Home PC
No Conditional Access rule, connection blocked
TeamViewer network
<i>Figure 3b</i></td></tr>
</table>

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 the TeamViewer Tensor Management 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

Key benefits **in a nutshell**

Increase IT security

Granular control

Mitigate risks

Boost efficiency

Greater flexibility

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.

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

Greater flexibility
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.

Without Conditional Access vs with **Conditional Access**

Without Conditional Access	With 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 if Conditional Access is not provisioned in the company.	IT administrators can block incoming and outgoing connections, so users can only connect to devices based on predefined rules.
✓ Approved, connection possible: Employee devices within the network (Figure 1a)	✓ Approved by rules, connection possible: Employee devices within the network (Figure 2a)
✓ Approved, connection possible: Customer devices outside the network (Figure 2a)	✓ Approved by rules, connection possible: Customer devices outside the network (Figure 2b)
✓ Unapproved, connection possible: Personal servers and devices at home (Figure 3a)	✗ Unapproved, no rules, connection blocked: Personal servers and devices at home (Figure 3b)

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