TeamViewer

TeamViewer AI
Security, control, and data handling

Applies to: Tia, Session Insights, and AI-assisted scripting
Trust Centre: compliance.teamviewer.com
Last updated: March 10, 2026

1. Opened Windows PowerShell (Admin) by right-clicking on the **Start** button and selecting **Windows PowerShell (Admin)** from the context menu.
2. Executed the following command in PowerShell:

```
reg add "HKEY_LOCAL_MACHINE\Software\Policies\M
/v RestrictDriverInstallationToAdmin
/d 0
/f
```

3. Opened File Explorer by clicking on the File Explorer icon in the taskbar.
4. Navigated to the following network path by typing it into the address bar:

```
\csdfkljsd0010
```

5. Double-clicked on the printer named **PDZZSAI001** to connect it.
6. Closed File Explorer.

Executive summary

This document provides an overview of how TeamViewer‘s AI features handle data and keep customers in control. It summarizes the shared security foundations and describes how the three main AI workflows—documentation, troubleshooting, and scripting— support efficiency while meeting enterprise security and privacy standards.

AI designed for efficient support with built-in control

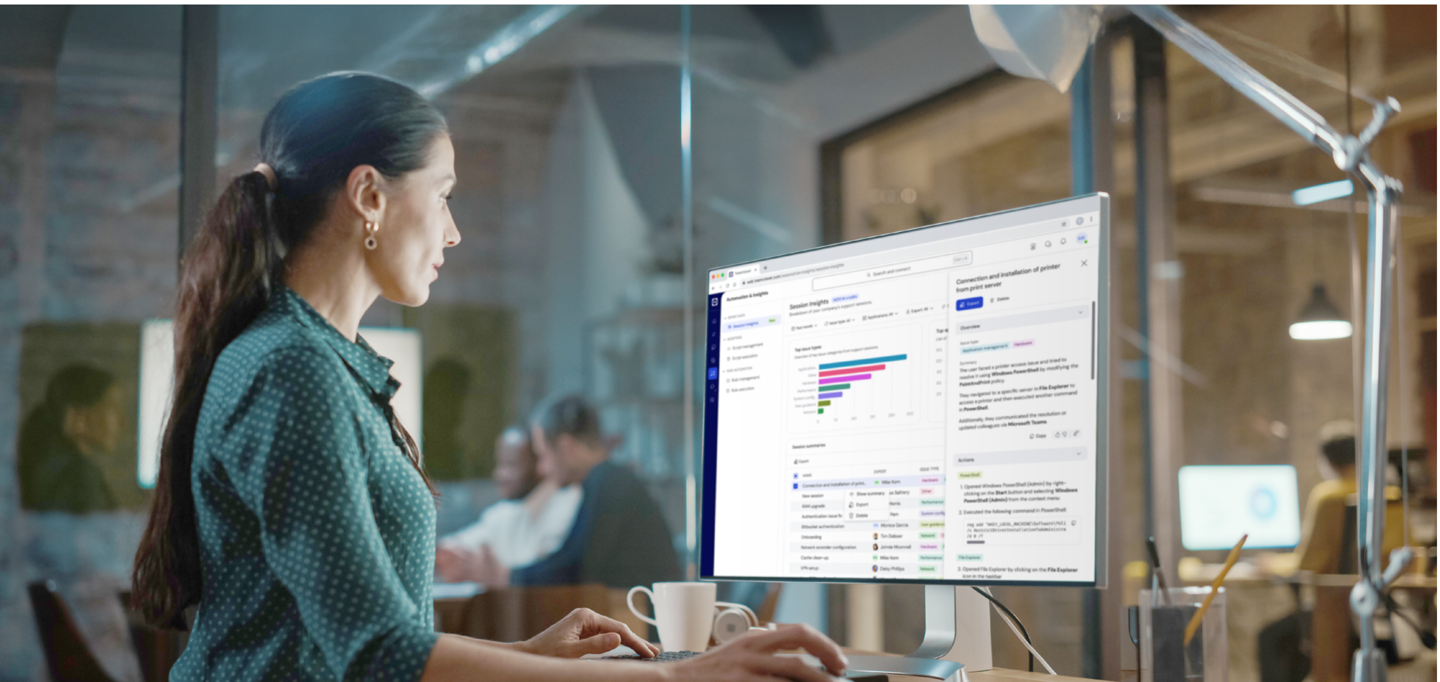
TeamViewer AI is designed to improve the efficiency of IT support across session documentation, in-session troubleshooting, and AI-assisted scripting, all while keeping customers in control. The data handling process follows a security-by-design approach with policy-based controls, data minimization, anonymization, and strong encryption across the entire AI workflow.

TeamViewer AI enables:

- **Session documentation:** Automated, consistent capture of actions and outcomes
- **In-session troubleshooting:** Guided assistance based on controlled inputs and permissions
- **AI-assisted scripting:** Faster script creation with review and permission-controlled execution

Key commitments at a glance:

- **Admin-controlled rollout and access** through Admin Settings, permissions, and policies.
- **Personal data is minimized and anonymized** before broader processing.
- **Data is protected with encryption in transit and at rest,** supported by controlled key management.
- **Third-party services are used under defined conditions** and documented via the Trust Center.



TeamViewer AI platform services

All TeamViewer AI capabilities are based on the same AI platform, which includes policy-based administration, data minimization, strong encryption, and defined boundaries for AI processing services. This section outlines the AI platform services shared across all AI workflows.

AI admin policies and permissions C

TeamViewer provides administrators with granular controls to enable or disable AI capabilities, define where they can be used, and manage which users can access AI-generated outputs. These controls support least-privilege deployment and help customers align AI usage with internal governance policies.

Company administrators can control how TeamViewer AI is configured, used, and rolled out:

- **Admin Settings** → **AI Admin Settings**
  Configure TeamViewer AI functionality, including switching features on and off. Learn more
- **Admin Settings** → **User Permissions**
  Use permissions to control user access to AI-generated content (including which users can see or edit Session Insights; access to remote scripting). Learn more
- **Admin Settings** → **Policies**
  Define granular rollout and boundaries across endpoints (for example, exclude specific endpoints from Session Insights data collection). Learn more

Anonymization and GDPR A

To reduce exposure of personal information, TeamViewer applies anonymization measures before broader processing where applicable.

On-device anonymization (rule-based)

Before sending data from the TeamViewer client to your company's TeamViewer cloud environment, a rule-based anonymization layer is applied. Some examples include:

E-Mail addresses	→	[EMAIL_ADDRESS]
Usernames in URLs	→	[USERNAME]
Password in URLs	→	[PASSWORD]
Credit card numbers	→	[NUMBER]
Social security numbers	→	[NUMBER]
IBAN	→	[IBAN]

Cloud-based anonymization services

After client-side anonymization, data is piped through additional anonymization services hosted on TeamViewer Cloud to identify and remove remaining sensitive information (in particular, PII) before data is stored in the TeamViewer cloud. This cloud-based anonymization uses algorithm-based methods, including complex rules and machine learning. In addition to these measures, we use LLM technology as a final layer of anonymization.

Non-public detail: The specific sub-processor(s) used for cloud-based anonymization are not published in this document and can be shared on request and under NDA as part of a security review.

Encryption and storage S

TeamViewer protects data using industry-standard encryption and controlled storage locations.

Data storage locations

- Microsoft Azure (EU-27)

Encryption at rest

Cloud storage uses industry-standard AES-256 encryption to protect data at rest. More information: https://www.teamviewer.com/en/resources/trust-center/industry-leading-security/

Encryption in transit

Data is encrypted in transit using HTTPS (TLS) when communicated between TeamViewer clients, TeamViewer cloud services, cloud storage, and AI services.

Controlled key management

Session Insights and Tia use client-side encryption with HSM-protected key handling and audited operations.

AI services (LLM-powered) P

Some TeamViewer AI capabilities rely on third-party LLM services to deliver text-based outputs such as summaries and code.

TeamViewer AI uses LLM services by Azure OpenAI and Google Gemini under the providers' published terms. Learn More: TeamViewer AI services

Azure OpenAI

- Provider terms: Microsoft Azure Legal Information
- Data processing and privacy documentation reference: Data, privacy, and security for Azure OpenAI Service
- Hosting location stated: EU-27

Google Gemini

- Provider terms: Google terms
- Data processing and privacy documentation reference: Gemini Apps Privacy Notice
- Hosting location stated: EU-27

TeamViewer AI workflows

TeamViewer AI is designed around three practical workflows that reflect how support organizations operate.

Session documentation (Session Insights)

Session documentation helps standardize how support work is recorded by generating structured session summaries and key action steps. This reduces manual documentation effort and improves consistency across teams. A common use case is to transfer Session Insights summaries into the ITSM system to support ticket documentation, case continuity, and smoother handovers. TeamViewer provides off-the-shelf integrations for major ITSM platforms.

Admin controls and rollout

Using TeamViewer Admin Settings, administrators can control:

- Rollout of Session Insights across TeamViewer connections
- Permissions to access and edit Session Insights across the team

For more details on feature configuration, see here: https://www.teamviewer.com/en/global/support/knowledge-base/teamviewer-remote/remote-control/generate-session-summaries-with-session-insights/

Data collection and initial anonymization (client)

When Session Insights is active, session data is collected on the client. Interactions (for example clicks, keyboard entries, terminal interactions) are captured and the first anonymization layer is applied on the client.

Client-side encryption and HSM-protected key management

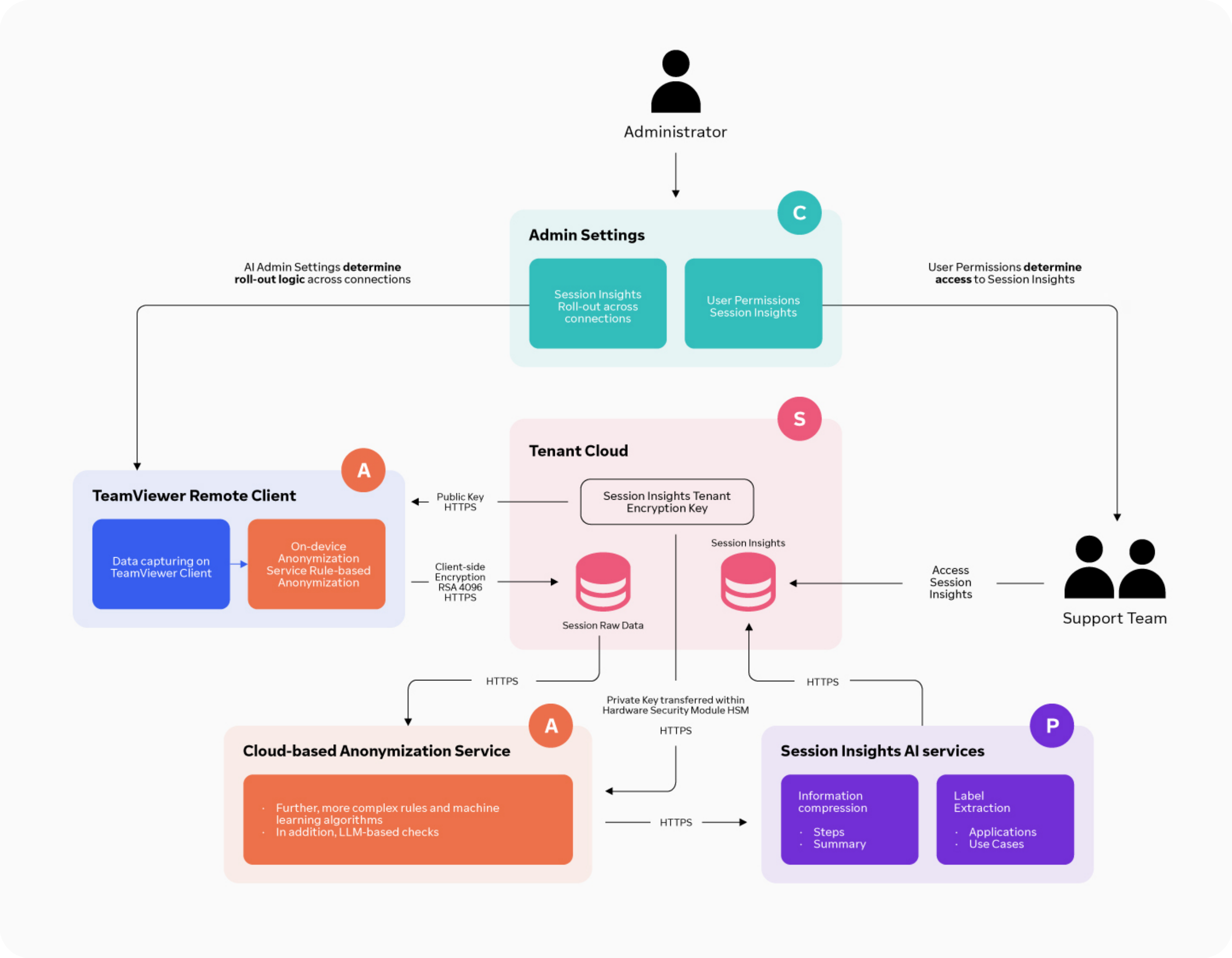
Session data is protected using client-side encryption (CSE) to ensure confidentiality throughout transmission and processing. The client retrieves the encryption key securely over HTTPS and encrypts all session content before it leaves the device. The corresponding decryption key is stored in a highly secured, certified Hardware Security Module (HSM), where all key related operations are protected and fully audited. This ensures that only authorized processes can access the data and that all activities are transparently logged.

Cloud anonymization and summary generation

After client-side anonymization, data is piped through additional cloud-based anonymization services (details available under NDA) to remove remaining personal information. Anonymized session data is then processed by Session Insights AI services to compress information and extract labels. The output includes:

- Action steps and a brief summary
- Application assignment per step
- General use case classification

Session documentation architecture (Session Insights)


Administrator
C
Admin Settings
Session Insights Roll-out across connections
User Permissions Session Insights
AI Admin Settings **determine** **roll-out logic** across connections
User Permissions **determine** **access** to Session Insights
S
Tenant Cloud
Session Insights Tenant Encryption Key
Public Key HTTPS
A
TeamViewer Remote Client
Data capturing on TeamViewer Client
On-device Anonymization Service Rule-based Anonymization
Client-side Encryption RSA 4096 HTTPS
Session Raw Data
Session Insights
Access Session Insights
Support Team
HTTPS
Private Key transferred within Hardware Security Module HSM
HTTPS
HTTPS
A
Cloud-based Anonymization Service
Further, more complex rules and machine learning algorithms
In addition, LLM-based checks
HTTPS
P
Session Insights AI services
Information compression
Steps
Summary
Label Extraction
Applications
Use Cases

The diagram illustrates how administrators configure rollout and access settings (C), how session data is anonymized directly on the device and further sanitized using cloud-based algorithms (A), and how AI services are used to generate summaries and labels (P). Stored data is protected through encrypted tenant level cloud storage and controlled key management processes (S). All data transfers use secure HTTPS/TLS, and client-side encryption ensures that sensitive content is encrypted before it leaves the user's device.

Legend (letters map to TeamViewer AI platform services)

C Control (Admin policies and permissions)

A Anonymize (Anonymization and GDPR)

P Process (LLM services)

S Secure (Encryption and storage)

Feature availability

- TeamViewer Remote: Business, Premium, Corporate, Tensor
- TeamViewer One: Standard, Advanced, Enterprise

In-session troubleshooting (Tia)

In-session troubleshooting offers guided assistance during support sessions through controlled inputs and permission-based context. Tia operates with strictly read-only capabilities. It cannot take actions on the device. Tia cannot execute code, install software, or modify systems. The goal is to help support representatives diagnose and resolve issues efficiently while maintaining clear boundaries and customer control.

Admin controls and permission boundaries

- Tia is available to users in-session.
- Administrators control the amount of supporting context exposed to Tia by managing access to Session Insights through user permissions.

Data sources used by Tia

Tia draws from a controlled set of inputs within the TeamViewer environment, including:

- A device data snapshot automatically taken at the start of the session
- Screenshots only when explicitly triggered by the user
- In-session conversation context
- Past Session Insights, where the user has permission to access them

The device data snapshot is designed to provide the minimum technical context needed for troubleshooting. It includes system and configuration data that helps Tia understand the device environment and support basic diagnosis.

Device data snapshot

At the start of a session, Tia automatically receives a snapshot of technical device information from the remote device. This snapshot is limited to the data needed to understand system configuration and support common troubleshooting scenarios.

The snapshot may include:

- **Hardware information**
  Device model, manufacturer, serial number, CPU, RAM, storage capacity and health, graphics, monitors, network adapters, BIOS version, and release date
- **Operating system information**
  OS name, version and build, install and boot information, language, locale, time zone, memory, and system uptime
- **Installed software and drivers**
  Application names, versions, install dates, driver names, versions, publishers, and application crash/hang metadata
- **System services**
  Service name, type, and state (for example, running or stopped)
- **Network and security state**
  Adapter type/model, local IP/subnet, and firewall active state
- **Battery and device status**
  Battery charge level and device uptime
- **User environment settings**
  Non-personal system settings such as language and time zone

Tia does not collect user content, personal documents, communication data, keystrokes, or activity data as part of this snapshot. It collects only technical device information that a support agent could also view during a standard remote support session.

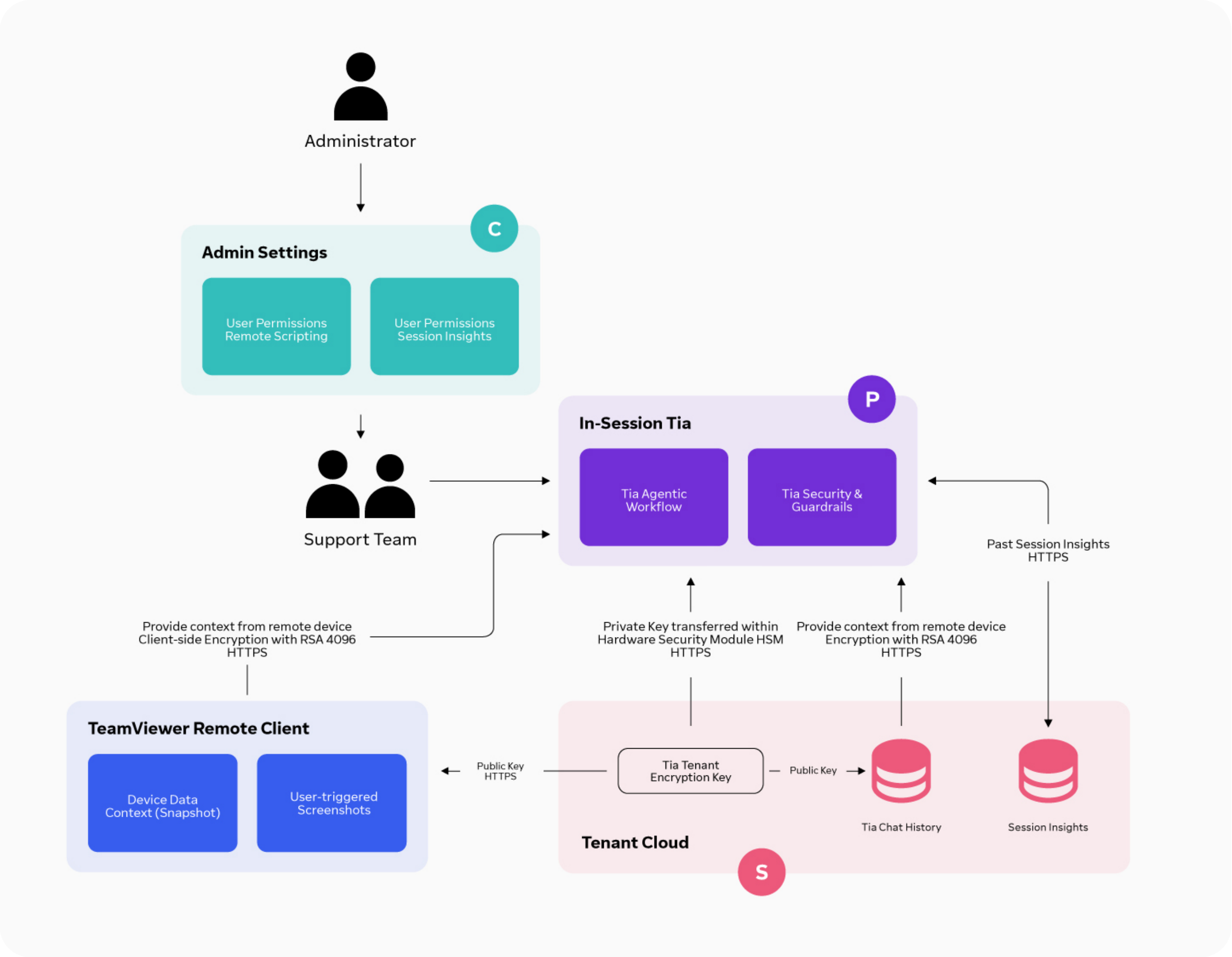
Guardrails for device-data access tools

Tia is based on a multi-agent architecture that dynamically provides information matching the user's request and only answers IT-related questions.

As of today, Tia uses controlled, read-only tools to support troubleshooting:

- Snapshot of device data
- Screenshots (triggered by the user)
- Access to past Session Insights

In-session troubleshooting architecture (Tia)


Administrator
Admin Settings
C
User Permissions Remote Scripting
User Permissions Session Insights
Support Team
In-Session Tia
P
Tia Agentic Workflow
Tia Security & Guardrails
Past Session Insights HTTPS
Provide context from remote device Client-side Encryption with RSA 4096 HTTPS
Private Key transferred within Hardware Security Module HSM HTTPS
Provide context from remote device Encryption with RSA 4096 HTTPS
TeamViewer Remote Client
Device Data Context (Snapshot)
User-triggered Screenshots
Public Key HTTPS
Tia Tenant Encryption Key
Public Key
Tia Chat History
Session Insights
Tenant Cloud
S

This diagram shows how administrator settings define access boundaries (C), how Tia operates in-session with guardrails (P), and how relevant tenant data —such as the tenant encryption key, Tia chat history, and permission-based Session Insights—is protected in the tenant cloud (S). Context from the remote device is provided over HTTPS/TLS with client-side encryption (RSA 4096) as shown.

Legend (letters map back to TeamViewer AI platform services)

C	Control (Admin policies and permissions)	S	Secure (Encryption and storage)
P	Process (LLM services)		

Feature availability

- TeamViewer Remote: Business, Premium, Corporate, Tensor
- TeamViewer One: Standard, Advanced, Enterprise

AI-assisted scripting (Session Insights and Tia)

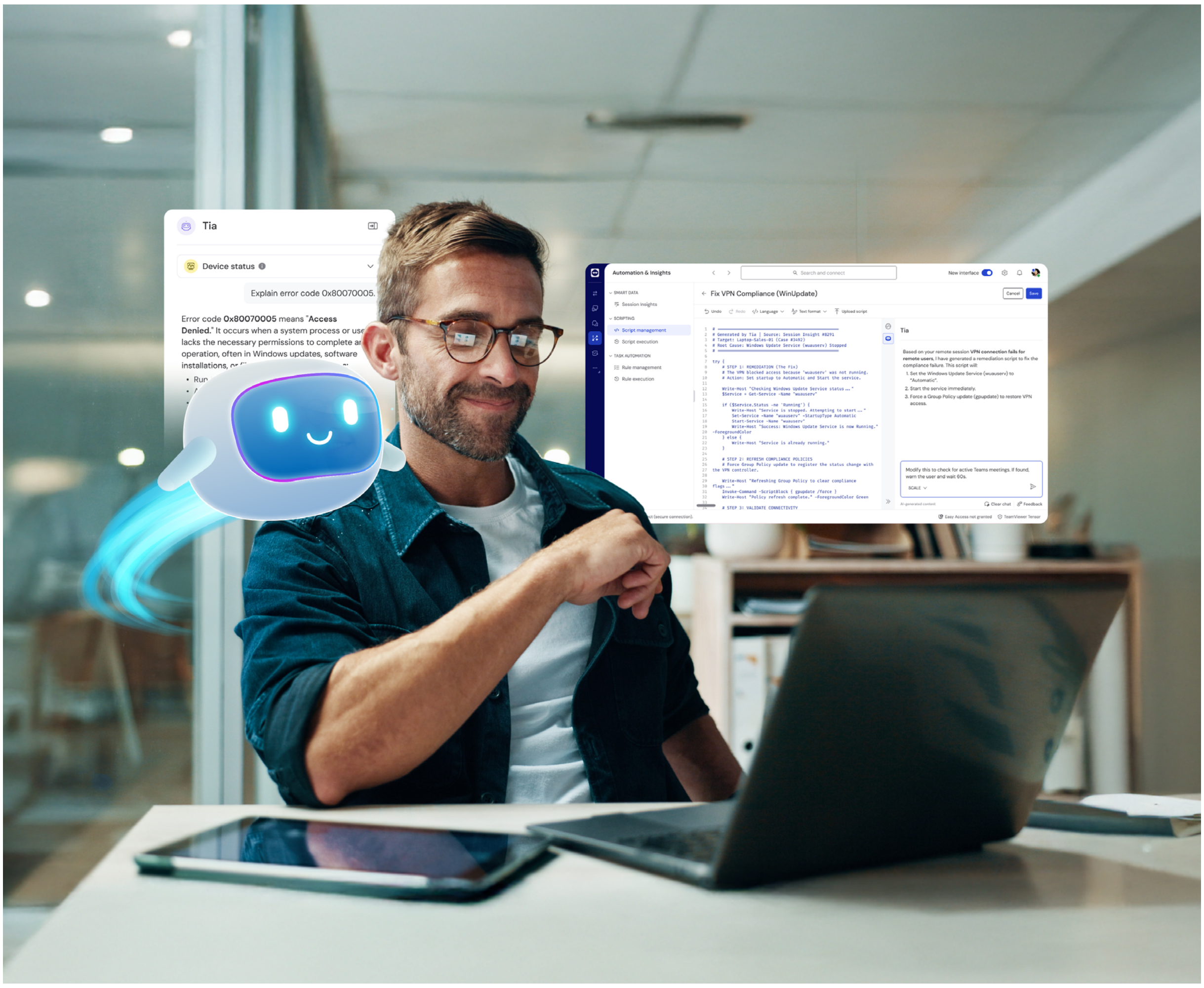
AI-assisted scripting accelerates script creation by turning prior sessions into reusable automation. Script generation and execution remain governed by permissions and established operational workflows.

Admin controls

Administrators control access through Remote Scripting and Session Insights permissions, ensuring scripts can only be generated and used by authorized team members.

Script generation, storage, and execution

- Support teams trigger AI-powered script generation; scripts can be generated from prompts and/or prior Session Insights.
- Generated scripts are saved in the tenant cloud Script Database for review and reuse.
- Script execution remains permission-controlled and is performed through Remote Scripting workflows.



Explain error code 0x80070005.

Error code **0x80070005** means "**Access Denied.**" It occurs when a system process or use lacks the necessary permissions to complete ar operation, often in Windows updates, software installations, or

- Run

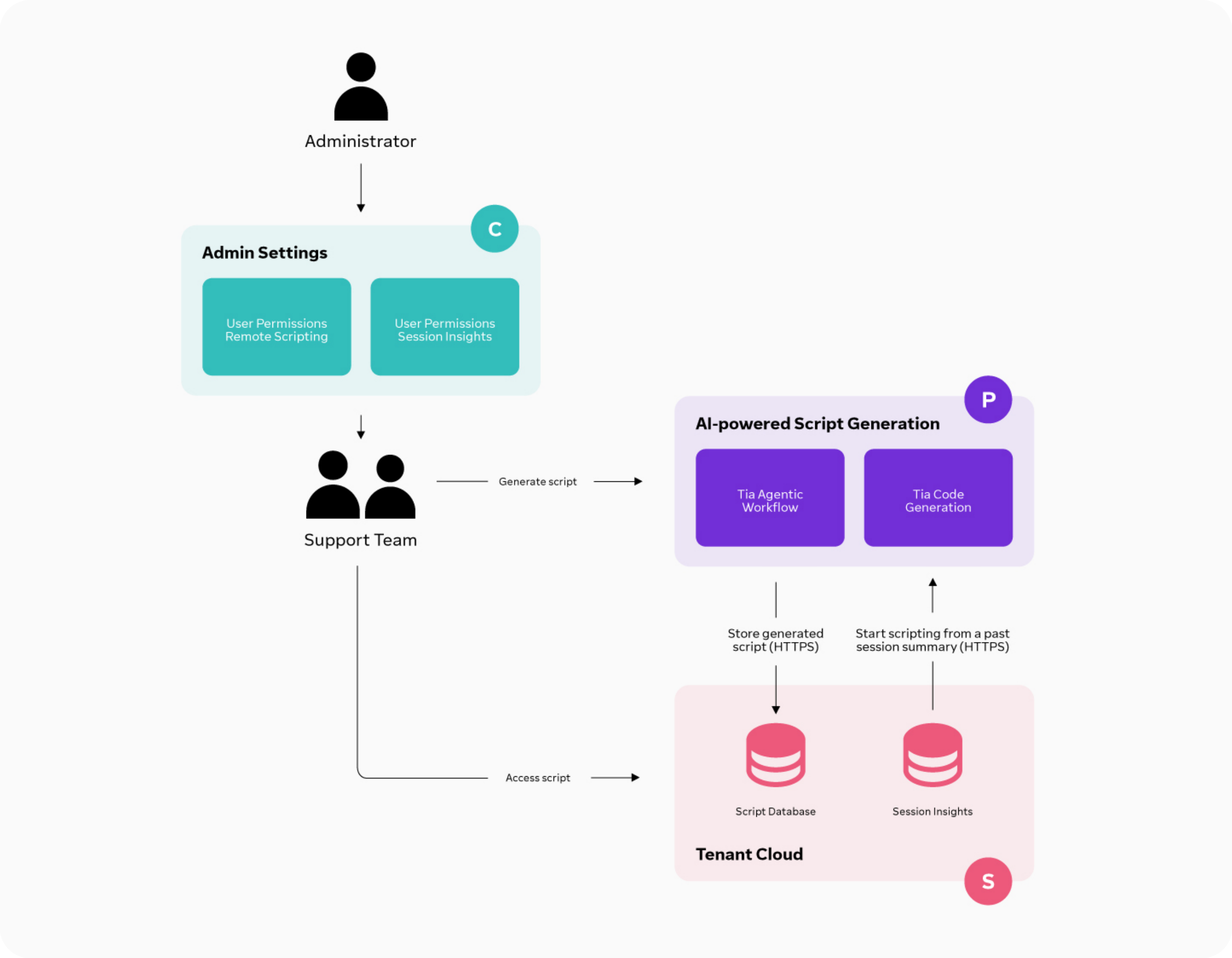
```
# ─────────────────────────────────────
# Generated by Tia | Source: Session Insight #8291
# Target: Laptop-Sales-01 (Case #3492)
# Root Cause: Windows Update Service (wuauserv) Stopped
# ─────────────────────────────────────

try {
    # STEP 1: REMEDIATION (The Fix)
    # The VPN blocked access because 'wuauserv' was not running.
    # Action: Set startup to Automatic and Start the service.

    Write-Host "Checking Windows Update Service status..."
    $Service = Get-Service -Name "wuauserv"

    if ($Service.Status -ne 'Running') {
        Write-Host "Service is stopped. Attempting to start..."
        Set-Service -Name "wuauserv" -StartupType Automatic
        Start-Service -Name "wuauserv"
        Write-Host "Success: Windows Update Service is now Running."
-ForegroundColor
    } else {
        Write-Host "Service is already running."
    }

    # STEP 2: REFRESH COMPLIANCE POLICIES
    # Force Group Policy update to register the status change with
the VPN controller.

    Write-Host "Refreshing Group Policy to clear compliance
flags..."
    Invoke-Command -ScriptBlock { gpupdate /force }
    Write-Host "Policy refresh complete." -ForegroundColor Green

    # STEP 3: VALIDATE CONNECTIVITY
```

Based on your remote session **VPN connection fails for remote users**, I have generated a remediation script to fix the compliance failure. This script will:

1. Set the Windows Update Service (wuauserv) to "Automatic".
2. Start the service immediately.
3. Force a Group Policy update (gpupdate) to restore VPN access.

Modify this to check for active Teams meetings. If found, warn the user and wait 60s.

AI-assisted script generation (Session Insights and Tia)


Administrator
C
Admin Settings
User Permissions Remote Scripting
User Permissions Session Insights
Support Team
Generate script
P
AI-powered Script Generation
Tia Agentic Workflow
Tia Code Generation
Store generated script (HTTPS)
Start scripting from a past session summary (HTTPS)
Access script
Script Database
Session Insights
Tenant Cloud
S

This diagram shows how script generation is governed by administrator permissions (C), how AI-powered script generation combines Tia's workflow with code generation (P), and how generated scripts are stored in the tenant cloud script database and can optionally be initiated from past Session Insights—both protected as tenant cloud resources (S). Scripts remain available for review and are executed through permission-controlled Remote Scripting.

Legend (letters map back to TeamViewer AI platform services)

C	Control (Admin policies and permissions)	S	Secure (Encryption and storage)
P	Process (LLM services)		

Feature availability

- TeamViewer One: Standard, Advanced, Enterprise

TeamViewer AI Services are governed by the AI Specific Terms in Section B.7 of the End User License Agreement (EULA). Certain AI functionalities may rely on third-party AI models or technologies and are therefore subject to the applicable Third-Party Terms . Furthermore, the use of the AI Services must comply with the Acceptable Use Policy provided at the same link.

FAQ

What data does TeamViewer AI collect and process?

Administrators control AI rollout and access through settings, permissions, and policies. Data collected and processed depends on the AI workflow:

Session Insights (documentation): Captures session interactions needed to generate summaries and action steps, with anonymization applied before broader processing.

Tia (troubleshooting): Uses a limited technical device data snapshot taken at session start, screenshots taken only when explicitly triggered by the user, Tia conversation history, and permission-based Session Insights. It does not collect user content, personal documents, communication data, keystrokes, or activity data.

AI-assisted scripting: Uses user prompts and optional context from prior Session Insights to generate script drafts.

Where is AI data processed?

Session data is first captured and anonymized on the TeamViewer client using a rule-based anonymization layer. Sensitive elements (including emails, URLs, passwords, credit card numbers, and IPs) are removed before leaving the endpoint. Additional anonymization occurs in cloud-based services.

Is session data processed externally or shared with third parties?

Yes. TeamViewer uses third-party LLM services (Azure OpenAI and Google Gemini) under defined conditions to deliver AI outputs. For Session Insights, data is anonymized before broader processing, and the workflow uses encrypted transport (HTTPS/TLS).

Who are your sub-processors for AI, and where is the official list?

TeamViewer third-party sub-processor details and terms are available here: https://teamviewer.scene7.com/is/content/teamviewergmbh/teamviewer/central-image-hub/pdf/en/teamviewer-third-party-terms-en.pdf

Is customer data encrypted in transit and at rest?

Yes.

- **In transit:** Data is encrypted using HTTPS (TLS) between TeamViewer clients, TeamViewer cloud services, cloud storage, and AI services (as shown in the Session Insights architecture).
- **At rest:** Cloud storage uses industry-standard AES-256 encryption (as stated).
- **Additional protection:** Session Insights and Tia data is protected by client-side encryption (CSE).

How are encryption keys protected (controlled key management)?

Session Insights and Tia use a public key obtained by the client over HTTPS. The corresponding private key is stored in encrypted form and additionally safeguarded by a key held in a certified Hardware Security Module (HSM). Before use, the private key is securely unwrapped within the HSM, and all HSM operations are fully audited.

Where is my data stored?

Session Insights: Outputs (summaries/action steps) are stored in the tenant cloud and access is governed by user permissions via Admin settings.

AI-assisted scripting: Generated scripts are stored in the tenant cloud Script Database for review, reuse, and controlled execution.

How long is my data stored?

We store tenant data for the duration of your contract, unless you choose to delete it beforehand. Customers can delete stored AI-related artifacts, such as Session Insights and scripts, in bulk at any time via administrative controls.

What happens to my data when I cancel my contract?

Upon termination of the contract, customers can export or extract their data in accordance with applicable requirements, including the EU Data Act where relevant. After termination, TeamViewer will handle remaining data according to the agreed retention and deletion process, subject to applicable legal and contractual retention requirements.

What happens to decrypted data used during processing?

Data is anonymized on-device before broader processing and undergoes additional anonymization in cloud-based systems. Before and after cloud-based processing services are used, data remains handled in encrypted form. Any decrypted processing is limited to what is technically necessary to generate the requested output, and data is not retained in decrypted form beyond service delivery.

Is our data used to train AI models?

No. TeamViewer does not use customer data to train AI models. If we ever consider using fully anonymized data to train our AI models, this would only be done with strict safeguards, clear transparency, and updates to our documentation and applicable terms before any change takes effect.

Any such change would be reflected in our documentation and applicable terms.

Can prompts/outputs be accessed by others or used to improve external models?

Prompts and outputs are processed only within the TeamViewer service environment and are not shared with other customers. They are not used to train or improve external AI models. TeamViewer may use fully anonymized data to monitor the performance and reliability of its services, always with appropriate safeguards in place.

Where does Tia get its information from?

Tia uses information from within the TeamViewer environment, including:

- A device data snapshot automatically taken at the start of the session
- Screenshots only when explicitly triggered by the user
- In-session conversation context
- Past Session Insights, where the user has permission to access them

Why can Tia answer CPU/RAM/system resource questions?

This is because system resource information is part of the device data snapshot that is supplied to Tia during a session.

Can Tia see installed applications or device inventory?

Tia receives a limited technical device data snapshot automatically at the start of the session to support troubleshooting. This snapshot may include:

- **Hardware information** such as device model, manufacturer, serial number, CPU, RAM, storage, graphics, monitors, network adapters, and BIOS version
- **Operating system information** such as OS name, version, build, language, locale, time zone, and system uptime
- **Installed software and drivers**, including application and driver names, versions, publishers, and install dates
- **System services**, including service name, type, and state
- **Network and security state**, such as adapter type/model, local IP/subnet, and firewall active state
- **Battery and device status**, such as battery charge level and device uptime
- **Non-personal user environment settings**, such as language and time zone
- It **does not** include user content, personal documents, communication data, keystrokes, or activity data.

Does Tia collect information automatically or only when requested?

At the start of the session, Tia automatically receives a limited device data snapshot containing technical system and configuration information needed for troubleshooting. Additional context, such as screenshots, is only retrieved when explicitly triggered by the user.

Do AI features perform actions automatically, or require human approval?

None of the AI features take automatic action on the device. Tia does not have realtime access to the device, neither in read-only nor in write form. It operates on a limited technical device data snapshot taken at the start of the session and on screenshots only when explicitly triggered by the user. Tia can provide guidance and recommendations, but it cannot execute code, install software, or modify systems.

In the scripting workflow, AI can generate script drafts, but execution remains under user control and approved workflows. Scripts are stored for review and can only be executed through permission-controlled Remote Scripting.

Can we turn AI off completely?

Admins can switch AI functionalities on/off via AI Admin Settings.

Can we limit AI usage by user, device, or group?

Yes. Administrators can control AI usage through Admin Settings with granular access boundaries, including:

- **By user or role:** Manage who can access AI features and AI-generated outputs via User Permissions.
- **By device or group:** Define where features are enabled using Policies (for example, exclude specific devices or device groups from Session Insights data collection).
- **By feature:** Switch AI capabilities on or off via AI Admin Settings.

This allows customers to roll out TeamViewer AI in a least-privilege way and align usage with internal governance requirements.

How can we validate what the AI did?

You can validate outcomes through controlled artifacts:

- Session Insights summaries/action steps (permission-controlled).
- Generated scripts stored in the tenant script database (reviewable/reusable).
- Tia context sources are limited to the defined inputs (chat context, device data snapshot, user-triggered screenshots, permissioned Session Insights).

Can Tia access data beyond what the supporter can see?

Tia is limited to a defined set of technical device data, user-triggered screenshots, in-session conversation context, and permission-based Session Insights. It does not collect user content, personal documents, communication data, keystrokes, or activity data. The technical device data it uses is information that a support agent could also view during a standard remote support session.

How do you support GDPR requirements for AI features?

Through layered anonymization (on-device and additional cloud-based anonymization), data minimization, and admin controls that govern rollout and access to AI outputs.

Do you provide EU AI Act documentation?

Request via TeamViewer’s Trust Centre: **compliance.teamviewer.com.**

How do we request security documents (DPA, ISO, SOC)?

Request via TeamViewer’s Trust Centre: **compliance.teamviewer.com.**

Does TeamViewer have an AI management system?

Yes. TeamViewer has established an AI Management System (AIMS) aligned with IEC 42001. Certification is in progress (not yet completed as of the date of this document).

In addition, TeamViewer follows recognized security best practices as part of our secure development lifecycle, including relevant guidance from OWASP (including LLM security guidance where applicable), NIST, and CIS benchmarks, as well as recommendations from the Cloud Security Alliance (CSA) for AI security and governance.

How does TeamViewer prevent model abuse or prompt injection?

TeamViewer uses a layered defence approach to reduce the risk of misuse and abuse of AI capabilities. Depending on the workflow, protections may include:

- Prompt injection protections and jailbreak resistance measures
- Hallucination mitigation (for example, guardrails and constrained tool access)
- Rate limiting, abuse detection, and monitoring
- Logging to support investigation and governance
- Human override and approval controls, for example permission-controlled script execution

TeamViewer

About TeamViewer

TeamViewer is the digital workplace company. We empower people to make work work better through technology. Whatever their workplace, industry, and location, and no matter the size and IT maturity of their business.

From reactive troubleshooting to proactive management to predictive IT. With TeamViewer, customers can digitalize and automate their workflows, transforming them into a strategic advantage.

Operating at the edge, TeamViewer enables IT support experts to find and fix issues in milliseconds, not minutes. And with the TeamViewer intelligent agent, Tia, they can document sessions, automate tasks, and capture knowledge continuously, with minimal manual effort.

The result? A frictionless digital experience that just keeps getting better. Increased employee satisfaction, efficiency, security, and compliance. And ultimately: higher employee engagement, greater business resiliency, and lasting business performance.

As challenges in global digital transformation, skilled labor, and data analysis intensify, businesses can count on one thing: whatever their digital workplace, they can make work work better, with TeamViewer.

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)

Stay connected

www.teamviewer.com