Prinect

Technical White Paper. Heidelberg TeamViewer for Remote Service.

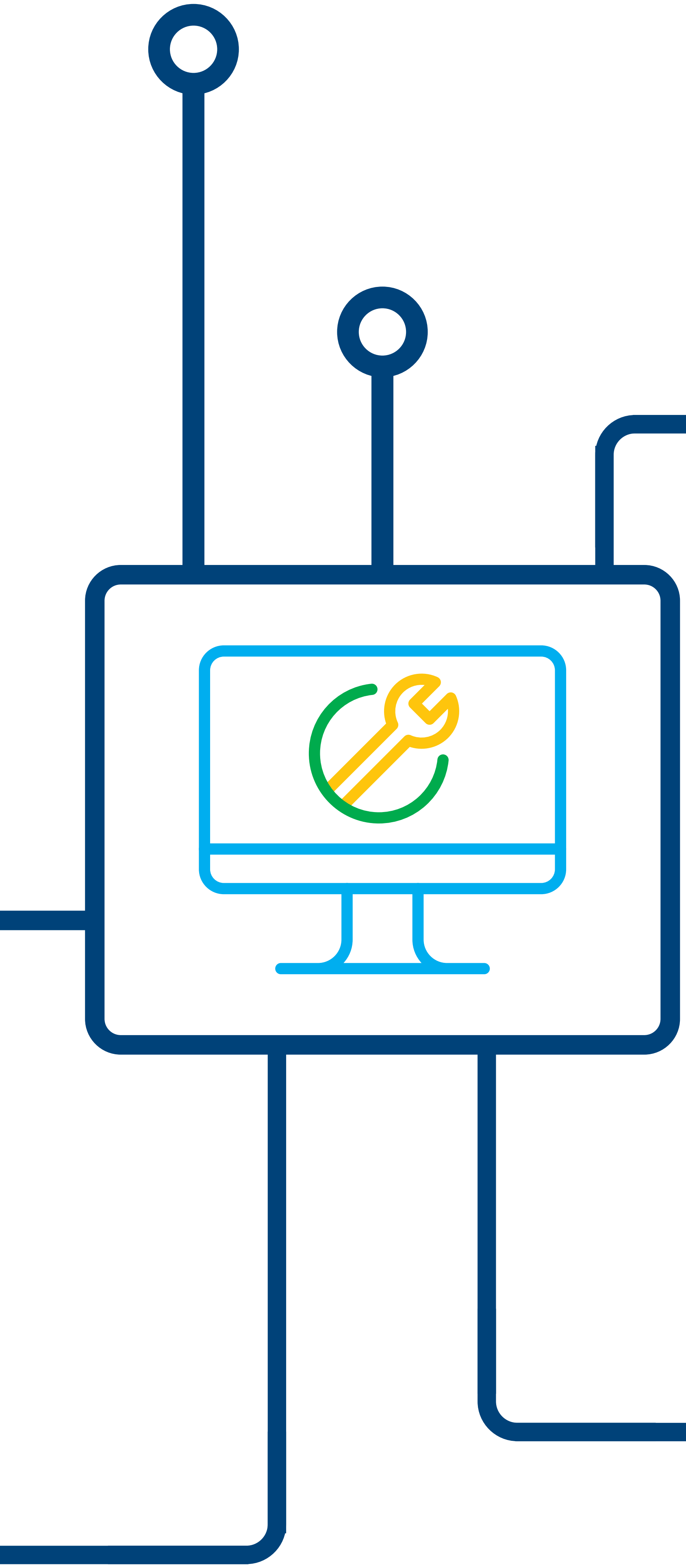
HEIDELBERG

Prinect.
TeamViewer Remote Service.

After an intensive review, Heidelberger Druckmaschinen (HDM) has chosen TeamViewer to partner with to provide secure Remote Help Desk support and Remote Installation/Upgrades for our Prinect® customers. TeamViewer is a market leader and their ability to provide private, encrypted, and secure remote access to Heidelberg® systems makes it an ideal tool for our world-class remote support services. The built-in high security features of TeamViewer Tensor coupled with an enterprise-class Conditional Access Router is why Heidelberg selected TeamViewer as their trusted partner. This white paper describes the use of TeamViewer to provide remote service and support to customers that require high security.

To view or download all of our Technical White Papers visit:
https://news.heidelbergusa.com/whitepapers/

Please note: The information provided herein is being delivered to you “as is” and Heidelberg makes no warranty as to its accuracy or use. Any use of the technical documentation or information contained herein is at the risk of the user.



Contents

TeamViewer.
As a company and software.

TeamViewer as Company and Software

TeamViewer GmbH was founded in 2005 and is based in southern Germany, in the city of Göppingen (near Stuttgart), with subsidiaries in Australia and the United States. They exclusively develop and sell secure systems for web-based collaboration. Within a short span of time, their "Freemium" licensing has led to rapid growth, with more than 320 million users of the TeamViewer software on more than 2.5 billion devices, in more than 200 countries around the globe. The software is available in more than 30 languages.

➔ Understanding of Security

TeamViewer is used by more than 30 million users at any given point in time. These users are providing spontaneous support over the Internet, accessing unattended computers (e.g., remote support for servers) and hosting online meetings. Depending on the configuration, TeamViewer can be used to remotely control another computer, as if one were sitting right in front of it. If the user who is logged on to a remote computer is a Windows®, Mac® or Linux administrator, this person will be granted administrator rights on that computer as well. Such powerful functionality over the potentially unsafe Internet must be protected against attacks with great scrutiny. In fact, the topic of security dominates all TeamViewer's development goals and is something we live and breathe in everything we do. We want to ensure access to your computer is safe and to protect our own interests: millions of users worldwide only trust a secure solution, and only a secure solution assures our long-term success as a business.

➔ Quality Management

Without an established quality management system, security management is not possible from TeamViewer's point of view. TeamViewer GmbH is one of the few providers on the market that practices certified quality management in accordance with ISO 9001. TeamViewer's quality management follows internationally recognized standards. TeamViewer has its QM system reviewed by external audits on an annual basis.

➔ External Expert Assessment

The TeamViewer software has been awarded a five-star quality seal (maximum value) by the Federal Association of IT Experts and Reviewers (Bundesverband der IT-Sachverständigen und Gutachter e.V., BISG e.V.). The independent reviewers of the BISG e.V. inspect products of qualified producers for their quality, security, and service characteristics.

➔ References

Currently, TeamViewer is used by more than 200 million users. This includes top International corporations from all kinds of industries (including such highly sensitive sectors as banking, finance, healthcare, government, and graphic arts industries that service these industries) are successfully using TeamViewer.

TeamViewer invites you to have a look at our references all over the Internet to gain first-hand impressions of the acceptance of our solution. You'll find that most other companies had similar security and availability requirements before they – after an intensive investigation – decided on TeamViewer. To form your own impression though, please find some technical details in the rest of this document.

Tensor security.

TeamViewer ensures security and transparency for all its customers by using end-to-end Encryption, where not even TeamViewer, as the operator of the routing servers, can read the encrypted data traffic (this is described below under “Secure Connection setup”). Heidelberg explicitly selected TeamViewer as an enterprise solution to ensure scalability and security for its customers.

Secure Connection Setup
When establishing a session, TeamViewer determines the optimal type of connection. After the handshake through our master servers (HDM chose for higher security TeamViewer Conditional Access router to handle the connections, more information in section 3), a direct connection via UDP or TCP is established in 70% of all cases (even behind standard gateways, NATs, and firewalls). The rest of the connections are routed through our highly redundant router network via TCP or https tunneling. Not even TeamViewer, as the operator of the routing servers, can read the encrypted data traffic.

If your Firewall supports Geo-IP Filtering, you must enable access to Germany where our Conditional Access Router is located. Geo-IP filtering allows you to block web traffic from entire countries to prevent hackers from attacking your Printing Plant.

Used Ports:

TCP/UDP PORT 5938

TeamViewer prefers to make outbound TCP and UDP connections over port 5938 – this is the primary port it uses, and TeamViewer performs best using this port. Your firewall should allow this at a minimum.

TCP PORT 443

If TeamViewer can't connect over port 5938, it will try next to connect over TCP port 443. However, our mobile apps running on Android™, iOS, Windows Mobile®, and BlackBerry® don't use port 443.

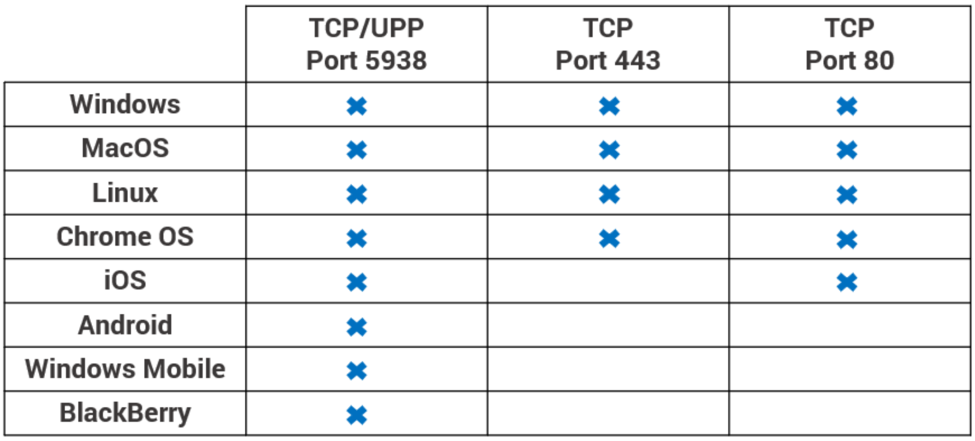
Note: port 443 is also used by our custom modules which are created in the Management Console. If you’re deploying a custom module, e.g., through Group Policy, then you need to ensure that port 443 is open on the computers to which you’re deploying. Port 443 is also used for a few other things, including TeamViewer update checks.

TCP PORT 80

If TeamViewer can’t connect over port 5938 or 443, then it will try on TCP port 80. The connection speed over this port is slower and less reliable than ports 5938 or 443, due to the additional overhead it uses, and there is no automatic reconnection if the connection is temporarily lost. For this reason, port 80 is only used as a last resort.

TeamViewer mobile apps running on Android, Windows Mobile, and BlackBerry don’t use port 80; however, the iOS apps can use port 80, if necessary.

Link: https://www.teamviewer.com/en/trust-center/security/?t=1632756123932#teamviewer-ports



	TCP/UPP Port 5938	TCP Port 443	TCP Port 80
Windows	✖	✖	✖
MacOS	✖	✖	✖
Linux	✖	✖	✖
Chrome OS	✖	✖	✖
iOS	✖		✖
Android	✖		
Windows Mobile	✖		
BlackBerry	✖		

Encryption and authentication.

To secure the transfer of data between points, two protocols are used: TLS and a proprietary encryption protocol.

TLS

TLS is used to secure connections to the Management Console. TeamViewer uses Version 1.2 and above. In addition, all connections between TeamViewers servers are run through TLS tunnels, even if the contained traffic is encrypted by other means.

Proprietary Encryption

TeamViewer traffic is secured using RSA public/private key exchange and AES (256-bit) session encryption. This technology is used in a comparable form for https/SSL and is considered completely safe by today's standards. As the private key never leaves the client computer, this procedure ensures that interconnected computers—including the TeamViewer routing servers—cannot decipher the data stream.

Each TeamViewer client has the Certificate of the master cluster and can thus verify certificates of the TeamViewer system. These certificates are used to establish a handshake between participants of the TeamViewer network.

A simplified overview of this handshake can be seen in the following diagram — **please refer to page 7.**

The session key derived from this handshake is afterwards used to encrypt the communication between parties using AES. In addition to this protocol, connections between TeamViewer servers run through a TLS tunnel.

For authorization and password encryption, Secure Remote Password protocol (SRP), an augmented password-authenticated key agreement (PAKE) protocol, is used. An infiltrator or man-in-the-middle cannot obtain enough information to be able to brute-force guess a password. This means that strong security can even be obtained using weak passwords; however, TeamViewer still recommends adhering to industry best practices for password creation to ensure the highest levels of security.

Each TeamViewer client has the public key of the master cluster implemented and can already encrypt messages to the master cluster and check messages signed by it. The PKI (Public Key Infrastructure) effectively prevents "man-in-the-middle-attacks" (MITM). Despite the encryption, the password is never sent directly, but only through a challenge-response procedure, and is only saved on the local computer. During authentication, the password is never transferred directly because the Secure Remote Password (SRP) protocol is used. Only a password verifier is stored on the local computer.

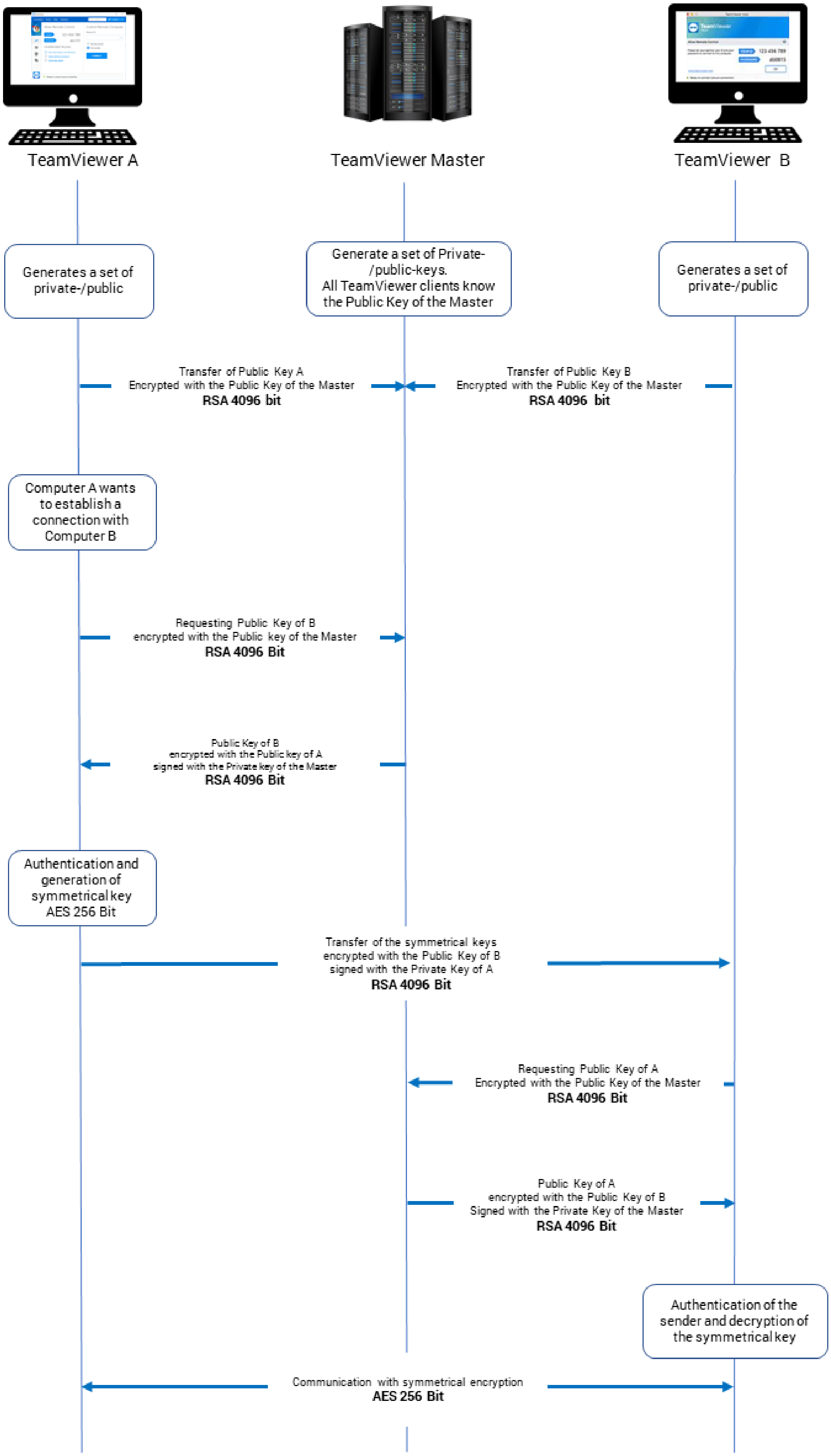
Brute Force Protection

Prospective customers who inquire about the security of TeamViewer regularly ask about encryption. Understandably, the risk that a third party could monitor the connection or that the TeamViewer access data is being tapped is feared most. However, the reality is that rather primitive attacks are often the most dangerous ones.

In the context of computer security, a brute-force attack is a trial-and-error-method to guess a password that is protecting a resource. With the growing computing power of standard computers, the time needed for guessing long passwords has been increasingly reduced.

As a defense against brute-force attacks, TeamViewer exponentially increases the latency between connection attempts. It thus takes as many as 17 hours for 24 attempts. The latency is only reset after successfully entering the correct password.

TeamViewer not only has a mechanism in place to protect its customers from attacks from one specific computer but also from multiple computers, known as botnet attacks, that are trying to access one particular TeamViewer-ID.


TeamViewer A
TeamViewer Master
TeamViewer B
Generates a set of private-/public
Generate a set of Private-/public-keys.
All TeamViewer clients know the Public Key of the Master
Generates a set of private-/public
Transfer of Public Key A
Encrypted with the Public Key of the Master
RSA 4096 bit
Transfer of Public Key B
Encrypted with the Public Key of the Master
RSA 4096 bit
Computer A wants to establish a connection with Computer B
Requesting Public Key of B
encrypted with the Public key of the Master
RSA 4096 Bit
Public Key of B
encrypted with the Public key of A
signed with the Private key of the Master
RSA 4096 Bit
Authentication and generation of symmetrical key AES 256 Bit
Transfer of the symmetrical keys
encrypted with the Public Key of B
signed with the Private Key of A
RSA 4096 Bit
Requesting Public Key of A
Encrypted with the Public Key of the Master
RSA 4096 Bit
Public Key of A
encrypted with the Public Key of B
Signed with the Private Key of the Master
RSA 4096 Bit
Authentication of the sender and decryption of the symmetrical key
Communication with symmetrical encryption
AES 256 Bit

TeamViewer encryptions and authentication

Validation of TeamViewer IDs

TeamViewer IDs are based on various hardware and software characteristics that are automatically generated by TeamViewer. The TeamViewer servers check the validity of these IDs.

Code Signing

As an additional security feature, all our software is signed via VeriSign Code Signing. In this manner, the publisher of the software is always readily identifiable. If the software has been changed afterwards, the digital signature automatically becomes invalid.

Datacenter & Backbone

To provide the best possible security and availability of the TeamViewer services, all TeamViewer servers are in ISO 27001-compliant data centers, leverage multi-redundant carrier connections and redundant power supplies. Furthermore, only state-of-the-art hardware is used. Additionally, all servers that store sensitive data are located within Germany or Austria.

Being ISO 27001-certified means that personal access control, video camera surveillance, motion detectors, 24/7 monitoring and on-site security personnel ensure access to the data center is only granted to authorized persons and guarantee the best possible security for hardware and data. There is also a detailed identification check at the single point-of-entry to the data center.

No Stealth Mode

There is no function that enables you to have TeamViewer running completely in the background. Even if the application is running as a Windows service in the background, TeamViewer is always visible by means of an icon in the system tray. After establishing a connection there is always a small control panel visible above the system tray. Therefore, TeamViewer is intentionally unsuitable for covertly monitoring computers or employees. This allows users to make sure that no sensitive data is shown on their screen during a TeamViewer session.

Security testing.

Both the TeamViewer infrastructure and the TeamViewer Software are subject to penetration testing on a regular basis. These tests are performed by independent companies that specialize in security testing. TeamViewer follows a modern DevSecOps approach — integrating all development, security, and operations processes — with a continuously improved Secure Software Development Life Cycle (S-SDLC). All TeamViewer software is protected against manipulation with DigiCert Code Signing.

Account Security

TeamViewer accounts are hosted on dedicated TeamViewer servers. For information on access control, please refer to Datacenter & Backbone above. For authorization and the Secure Remote Password (SRP) protocol version 6 is used. This protocol combines the advantages of conventional ways of password storage. We do not store any information on our servers that could be used by an attacker to authenticate as the given account. In addition, passwords are never sent to our servers during the authentication. Instead, a proof is used that is only valid for the single authentication run and can't be reused afterwards.

Stored Data

Personal data in accounts is stored encrypted. The encryption keys used for that are protected with a key that is directly derived from the Account password. The data itself is protected by a series of RSA and AES keys. These mechanisms are used for a wide variety of data such as passwords, chat and chat logs, backups, etc. This information is only decrypted on the client, or in the Management Console after the user logged in. Other services do not have access to user data. Together with the fact that no password or password equivalent data is stored in our databases, this prevents attackers from accessing user data.

Single Sign On

Using TeamViewer's Single Sign-On (SSO), Heidelberg reduces the user management efforts by connecting TeamViewer with our identity providers and user directories.

In general, SSO adds the following benefits:

- Mitigate risk for access to 3rd-party sites because passwords not stored or managed externally
- Reduce password fatigue
- Reduce time spent re-entering passwords
- Simpler administration
- Better administrative control
- Improved user productivity
- Eliminating multiple passwords, also reduces a common source of security breaches – users writing down their passwords, too weak password or always the same password.
- Administrator can know with certainty that when she/he disables a user's account, the account is fully disabled.

Link: **https://community.teamviewer.com/English/kb/articles/30784-single-sign-on-sso**

Active Directory/Azure AD Integration

Heidelberg centrally manages our Support Technicians within our Active Directory keeping our TeamViewer accounts automatically up to date. This provides account security by ensuring only active Heidelberg employees can use TeamViewer and deactivates employee accounts that are no longer needed.

Connection Possibility

TeamViewer has two types of connections: attended or unattended.

➔ **Attended –** is when, at least, one person at the customer's site must be in front of the device to initialize the connection for the Heidelberg Support Technician to be able to connect.

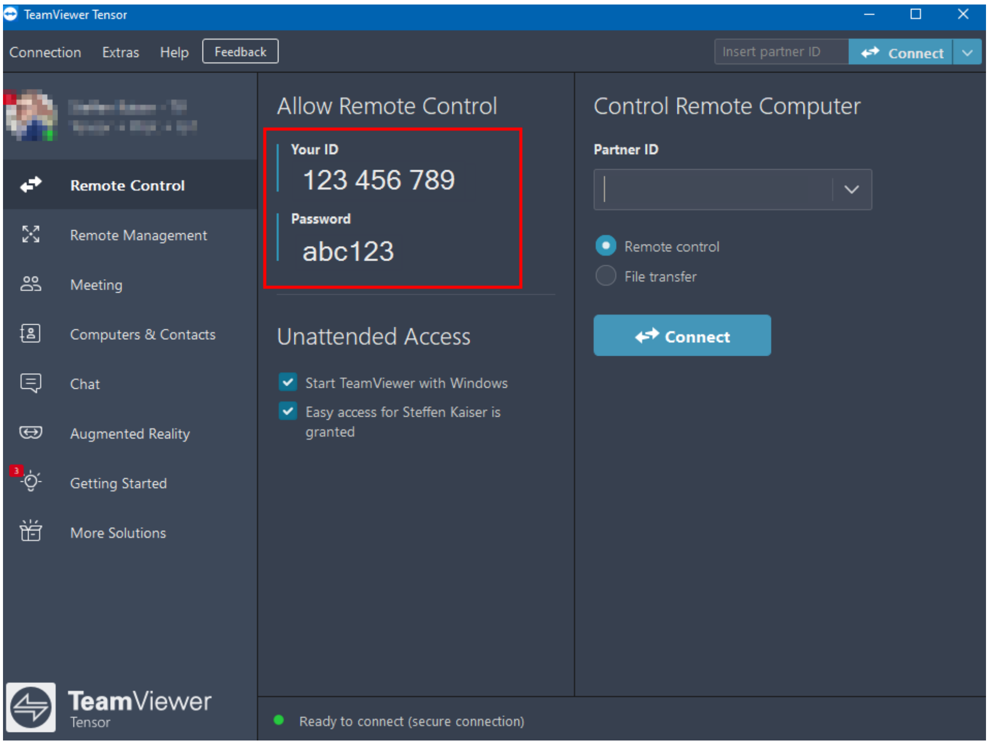
➔ **Unattended –** is when a Heidelberg Support Technician can connect even when no one from the customer's site is there to accept or initialize the incoming connection.

Heidelberg has decided to only use "Attended" access for connection to our customer's devices. You can enforce attended access with Conditional Access options. So, the "Unattended" access feature will be disabled via TeamViewer policy in our implementation. The following displays the different options for attended access.

TeamViewer ID + Password.

A TeamViewer ID is a unique numeric ID assigned to each device when TeamViewer is installed. This ID is designed not to change and should remain constant even if the software is uninstalled and reinstalled. Think of this ID like a phone number for your device. You dial the TeamViewer ID, then use the password to authenticate the connection.

Additionally, each TeamViewer Client has as default setting, a random password (see below) to initialize the connection. As it is random, the User in front of the device must let the Supporter know the password, which ensures attended access.



[redacted]

Allow Remote Control

Your ID
123 456 789

Password
abc123

Unattended Access

☑ Start TeamViewer with Windows
☑ Easy access for Steffen Kaiser is granted

Control Remote Computer

Partner ID

● Remote control
○ File transfer

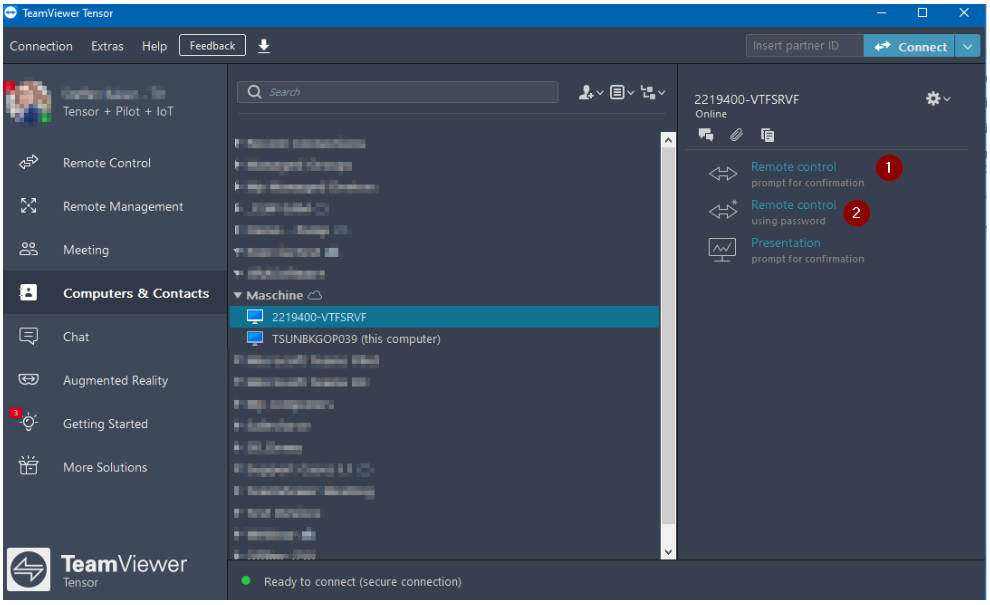
Connect

Ready to connect (secure connection)

Link: https://community.teamviewer.com/English/kb/articles/49515-what-is-a-teamviewer-id#teamviewer-id

Computer & Contacts (Groups)

Computer & Contacts list contains your groups of devices and contacts. These groups can be shared with colleagues to organize accordantly the company structure (https://community.teamviewer.com/English/kb/articles/30221-sharing-groups). In the Computer & Contacts list you can initialize the session via password or confirmation. Minimum permission will be granted to the Heidelberg Support Technician with segregated access. This ensures role-based access, only the needed people will have the possibility to see the group for initialization of the connection.



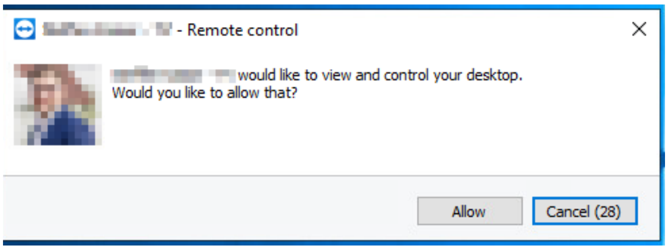
Password

The password option allows the use of TeamViewer in a similar way to using a TeamViewer Partner ID. The difference is that the ID is already known and saved. The need for a password ensures the attended access.

Link: https://community.teamviewer.com/English/kb/articles/28442-all-about-passwords#password-for-spontaneous-support

Confirmation

The Confirmation possibility enables the Heidelberg Support Technician to initialize a session with no other communication channel, as the customer only needs to accept the request. For the customer, this option will clearly identify the request for connection as well how we want to connect. The Confirmation can be accepted or declined by our customer. If the Confirmation is not accepted or declined, the request will timeout after 30 seconds and the connection will be declined.


- Remote control

would like to view and control your desktop.
Would you like to allow that?

Sessioncodes

Sessioncodes are mainly used to connect with a QuickSupport for instant, fast Support to devices not managed.

Link: https://community.teamviewer.com/English/kb/articles/49515-what-is-a-teamviewer-id#session-code-sxx-xxx-xxx

Policies

TeamViewer Policies are defined, distributed, and enforced setting policies for the TeamViewer software installations on devices that belong specifically to them. Heidelberg can centrally administrate the Policies within the TeamViewer Management Console. Setting policies are digitally signed by the account that generates them. This ensures that the only account permitted to assign a policy to a device is the account to which the device belongs. A full overview of possible policies is listed here:

Link: https://community.teamviewer.com/English/kb/articles/4860-how-to-add-a-new-settings-policy

Incoming and Outgoing Access Control

You can individually configure the connection modes of TeamViewer. For instance, you can configure your remote support or meeting computer in a way that no incoming connections are possible. Limiting functionality to those features needed always means limiting possible weak points for potential attacks. Additionally, it can be controlled via Conditional Access rules and options.

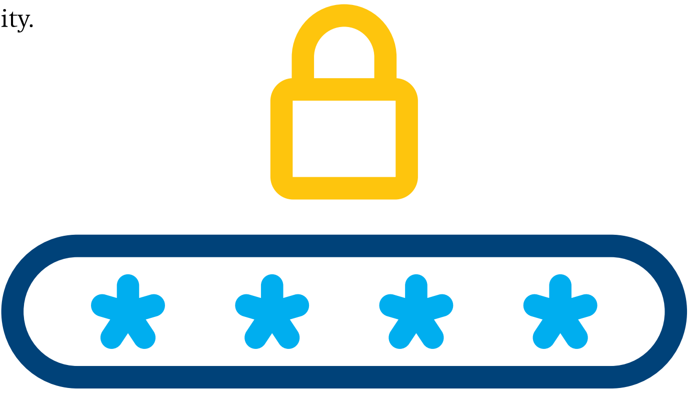
Password Strength

This configures the strength of the TeamViewer password (6, 8 or 10 characters) or even disables the random password as connection possibility.

Random password for each session

This enables TeamViewer users to decide for the use case if:

- The new password will not be generated until TeamViewer is restarted.
- TeamViewer generates a new password after each completed session.
- A password is generated only once.
- TeamViewer asks you after each session whether you would like to generate a new password.



TeamViewer Tensor™ Certificate

TeamViewer has the following certification to ensure high security for its customers and their customers:

Data Centers: ISO27001
HIPAA
SOC3
TISAX
ISO 9001:2015
Code Signing

The up-to-date general security information, certification and security guidelines can be accessed at:

https://www.teamviewer.com/en/trust-center/compliance/
https://www.teamviewer.com/en/trust-center/security/?t=1630344425332
https://community.teamviewer.com/English/kb/articles/108686-welcome-and-introduction

Online Resources

Visit the following pages to learn more about the functions and possibilities provided by TeamViewer Tensor:

- **TeamViewer Community:** https://community.teamviewer.com/English/
- **TeamViewer Knowledge Base:** https://community.teamviewer.com/English/kb
- **TeamViewer Trust Center:** https://www.teamviewer.com/en/trust-center/security/

Conditional Access.

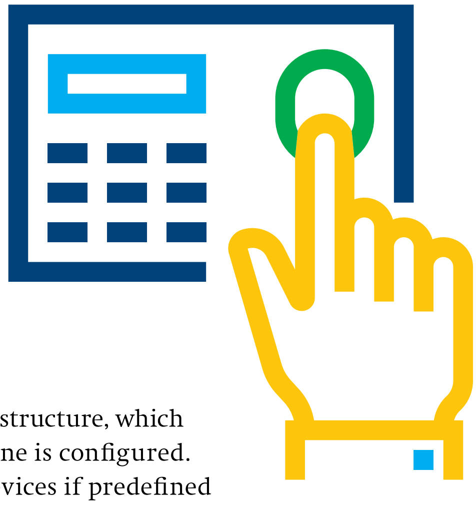
Conditional Access (CA) is the ultimate tool to ensure a state-of-the-art security and gives Heidelberg absolute control over who can use TeamViewer and which devices are allowed/blocked to use TeamViewer within the Heidelberg Corporate Network. It offers us the possibility to have a dedicated router that will work as a kind of firewall and determine all permissions within our network. This router works with Whitelisting philosophy. The main idea is to block all connections/use of TeamViewer in our network and allow who and which devices can connect to which account/device within our network.

General

With Conditional Access, Heidelberg controls the TeamViewer usage and access rights throughout our organization using a rules engine we configure within the Management Console. This conditional access provides an additional layer of security as well as prevents unauthorized remote access to our customer's Printing Plants, with a rule-based engine controlling permissions at the account, group, and device level. Conditional Access is a security feature and, therefore, no connection is allowed initially as soon as the rule verification is activated. With TeamViewer Tensor Conditional Access, Heidelberg can maintain company-wide oversight of TeamViewer access and usage from a single location.

TeamViewer Tensor Conditional Access enables Heidelberg to

- Centrally manage and control permission settings for TeamViewer features with associated access rights at the account, group, and device level.
- Define and enforce account and device access rights for remote control sessions.
- Prevent unauthorized remote connections to comply with corporate security policies
- Protect network perimeter access with a dedicated infrastructure, provided and maintained by TeamViewer

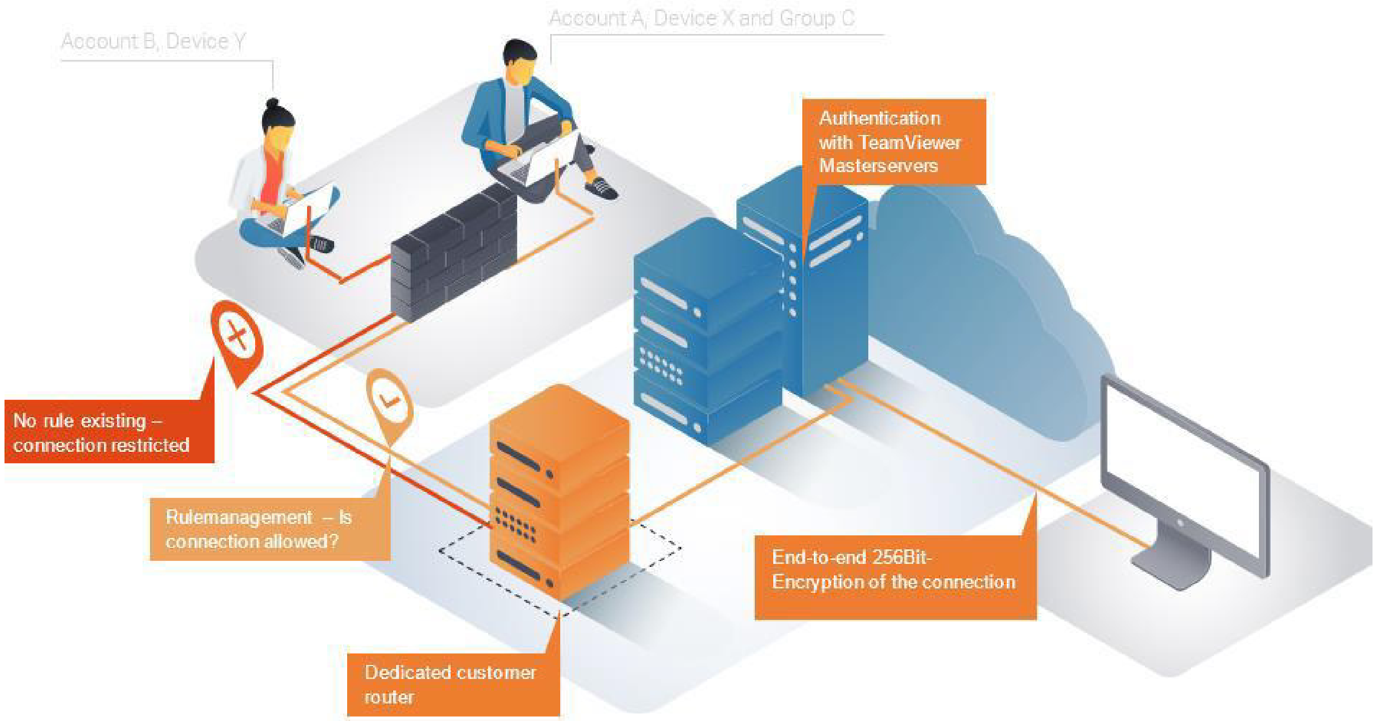


How does Conditional Access work?

TeamViewer provisions and maintains our Conditional Access infrastructure, which acts like a firewall that can be activated when its rule-based engine is configured. When activated, it authorizes access for accounts, groups, and devices if predefined conditions in the rule-based engine are met. If rules are inactive, such as during initial setup or maintenance, Conditional Access can be deactivated, which blocks all incoming TeamViewer connection attempts.

In the Management Console, Heidelberg can:

- Set defined maintenance windows and time-slots for connections
- Manage and define remote access rules for accounts, groups, and authorized computers (Windows and MacOS), also Mobile Devices and Assist AR can be used with CA
- Assign who controls TeamViewer user rights and permissions
- Set required conditions to authorize access rights and access control for users, groups, or network devices


Account B, Device Y
Account A, Device X and Group C
Authentication with TeamViewer Masterservers
No rule existing – connection restricted
Rulemanagement – Is connection allowed?
End-to-end 256Bit-Encryption of the connection
Dedicated customer router

To activate Conditional Access, rules are defined in the Management Console based on account, group, or device. This central and global rule management is independent from the device configuration and provides Heidelberg with the ability to block or authorize usage within our corporate network or from outside locations.

- To establish connections, each customer is assigned dedicated hardware within the TeamViewer infrastructure that no other customers can access.
- TeamViewer Tensor Conditional Access blocks all TeamViewer access by default to maintain the highest security levels. You can set up your custom access rules within the Management Console to align with your company's security standards.
- Once the setup is complete, all connection attempts flow through the dedicated hardware and rule engine. Unauthorized users or devices will not be able to connect anymore.
- The engine will allow connections based on the rules you have set up. If a rule cannot be found, it will not allow connections to be established.

Overall, Heidelberg gains full control over remote connections within our corporate environment. This TeamViewer Tensor functionality helps us tighten up your security by allowing access and connections to only authorized users or devices, consequently preventing data leaks, risky behavior, and minimizing risks.

Key benefits.
For your organization.

- Keep your network perimeter protected from unauthorized remote access attempts
- Enable employees, consultants, and vendors to work remotely with secure access to authorized network systems, computers, and devices
- Boost productivity and operational efficiencies with centralized management and control of all connections and user access rights
- Leverage cloud scalability to manage thousands of devices, users, and connections
- Enforce and comply with corporate security policies
- Prevent unauthorized file transfers to external destinations
- Cut costs by eliminating expensive on-premises appliances
- Reduce the total cost of ownership with a cloud infrastructure – provided by TeamViewer
- Dedicated infrastructure without the burden of managing it – serviced by TeamViewer

Overall, you gain full control over remote connections within your printing plant.

Further always up-to-date information:

- **https://community.teamviewer.com/English/kb/articles/108699-conditional-access**
- **https://community.teamviewer.com/English/kb/articles/57261-get-started-conditional-access**

Summary:

Heidelberg's world-class support services continue to improve with the addition of TeamViewer to provide secure remote desktop capabilities. With TeamViewer Tensor and Conditional Access, we ensure highly secure connections integrated with the Heidelberg Prinect Workflow.

Please direct any questions regarding this document to Eugene F. O'Brien,
Senior Technical Support Analyst at: **(770) 794-6205 or eugene.obrien@heidelberg.com**

Heidelberg USA
1000 Gutenberg Drive
Kennesaw, GA 30144
Phone 800 437 7388
info@heidelberg.com
heidelberg.com/us

Subject to technical modifications and other changes.