Wolters Kluwer

TeamMate®

TeamCloud

TeamMate AM

Technical and Security Overview

Product Version:

TeamCloud TeamMate AM 12.0

Last Updated: March 21, 2017

Table of Contents

Introduction to TeamCloud

What is TeamCloud?

TeamCloud, TeamMate's hosting service, provides a secure access to your custom TeamMate environment over the web. Hosting can be a cost-effective alternative, providing a powerful and stable environment without the burden of deploying software and developing the associated infrastructure. Choosing TeamCloud allows your organization to concentrate on building your business, not your infrastructure.

Availability

With TeamCloud, your data is available when you need it. Your information resides on our managed servers, which are load balanced to provide maximum performance and stability. Your employees access your audit programs, work papers, recommendations, and other TeamMate data securely through the web. In today's information technology environment, employees expect web access to their tools. TeamMate Hosting solutions allow you to support your remote and local teams with the same flexible, stable environment.

Cost Savings

Your organization can achieve significant savings by letting us host TeamMate. Most organizations find that the cost of a hosted solution versus developing their own environment is significantly lower. The need to purchase and manage additional hardware as your TeamMate databases expand is eliminated. In addition, the involvement of your information technology staff is minimized, since our team fully supports user access, manages the servers, and monitors performance. TeamMate Hosting solutions are a cost-effective and flexible answer to the needs of many organizations. TeamMate software is not loaded on any of the customer's computers or servers.

Secure Solution

With TeamCloud, your information is protected and secure from physical risks and unauthorized access. Industry standard firewall, backup, and data center security technologies and processes are in place to keep your data available and secure.

TeamMate products available via TeamCloud

All current TeamMate products are available in TeamCloud, this document refers to TeamMate AM only.

Features

With TeamCloud TeamMate Hosting, we provide access to TeamMate customers via the Internet. TeamMate software is not loaded on any of the customer's computers or servers (Desktop requirements are listed later in the document).

Supported Browsers

As TeamCloud is always updated to the latest TeamMate version, please refer to the latest TeamMate AM IT Overview Document for latest web browsers supported.

NOTE: With TeamMate version R12 we have added support for Chrome and Edge browsers.

IMPORTANT: Access to the TeamCloud portal to run the desktop apps (EWP, TeamAdmin, etc.) will still require Internet Explorer. Chrome and Edge are not supported to access the TeamCloud Portal. TeamMate websites, TeamCentral, TEC, etc. will work with IE11, Chrome and Edge.

About this Document

We understand that privacy and security are of paramount importance to our customers and potential customers and we are committed to providing you with a secure application and environment. This document is made available to our customers and prospects to explain the TeamCloud security program and security infrastructure.

Intended Audience and Scope

This document is intended for the information security and privacy professionals of TeamMate customers and potential customers who need to know the technical details of the TeamCloud infrastructure and security program.

Confidentiality Agreements

This document may only be shared with TeamMate customers and potential customers who are subject to TeamMate's binding confidentiality terms. The recipient is not permitted to distribute or make available this document or any of its contents to any third party without the express written permission of TeamMate. Anyone else must immediately destroy all copies in their possession.

Customer Responsibility

TeamCloud allows our customers to control access rights, data collection, privacy policies, and terms of use for their environment(s). Customers are responsible for ensuring their collection and use of data in their environment(s) complies with their own privacy policies and all applicable laws.

TeamCloud applications process data in a content-agnostic manner, meaning that we do not know whether the data we are processing is personally identifiable information, confidential information, or otherwise.

Information is subject to change

This document reflects the state of TeamCloud as of the date listed on the cover page. Because technology is dynamic and ever changing, TeamMate reserves the right to change its processes, procedures, and tools as listed herein in connection with our ongoing effort to improve our hosting facilities, operations, and security.

Additional Sources of Information

Product Documentation

TeamMate product documentation, User Guides, and IT Overview documents are available on TeamMate Connect, https://services.teammateconnect.com/teammate-user-guides.

Privacy

Privacy Laws and Compliance

TeamCloud technical operations group, security team and legal department work closely together to ensure protection of customer data and TeamMate compliance with applicable privacy and other laws.

TeamMate Access to Customer Data

Access to customer data is strictly controlled and is only granted to select and authorized members of TeamCloud operations. All other Wolters Kluwer and TeamMate staff, including Support, Development, and Quality Assurance teams have NO access to TeamCloud Production environments. Any access to customer data by non-TeamCloud operations staff will require prior written authorization by the client first.

Customer data is not used in the Quality Assurance process without prior written customer consent.

Geographic Locations of Data Centers

Depending on where a client is geographically located, you can choose the location where your data is located. All customer data is backed up in the same region in which it is hosted. For example, customer data hosted out of the London data center is backed up and does not leave the UK.

All TeamCloud data center providers are SSAE 16 SOC2 (previously SAS-70) and ISO27001 certified.

Americas

- Dallas, Texas, USA, provided by Rackspace (DFW1)
- Toronto, Ontario, Canada, provided by CenturyLink (TR3)
- Washington D.C. Area, USA, provided by Datapipe (FedRAMP faculty)

Europe

- London, United Kingdom, provided by Rackspace (LON3)
- Q2/Q3 2017 we plan to have a Data Center in Germany

AsiaPac

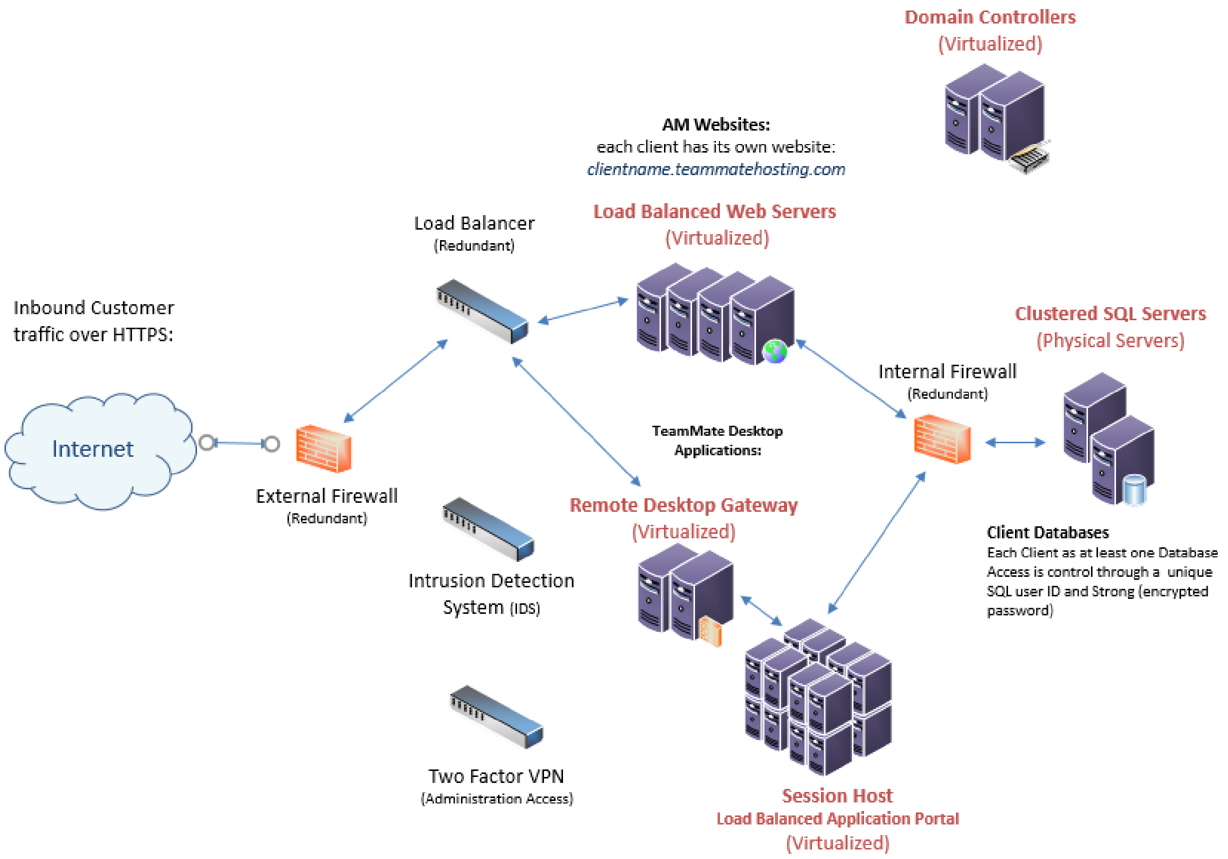
- Sydney Australia, provided by Rackspace (SYD1)

Data does not “move” between jurisdictions. Data is isolated to a specific data center/jurisdiction and is not copied anywhere else. No data stored with TeamCloud will be hosted outside of the customer’s region, although it may be accessed by TeamCloud operations staff in other locations to provide maintenance and support.

Network Architecture

The following diagram provides an overview of the TeamCloud network architecture. The TeamCloud production network, where customer data travels, is completely separated and segregated from the Wolters Kluwer corporate networks.

Extensive use of Microsoft Remote Application Server and IIS is used to provide TeamCloud; no software needs be installed on client PCs.



Client Databases
Each Client as at least one Database
Access is control through a unique
SQL user ID and Strong (encrypted
password)

Network Redundancy

Each data center uses multiple Internet feeds from multiple providers ensuring that in the event of a carrier outage, TeamCloud services will still be available. All relevant components of the data center operations and the TeamMate Hosted Software Solution are configured in N+1 redundancy, allowing all primary systems to suffer failures without interrupting service to the customer.

HTTPS Encryption

All data in transit is encrypted with a 256 bit TLS Certificate. No data leaves any of our data centers unencrypted.

Additional Network Controls

DDoS Detection

Distributed Denial of Service (DDoS) Monitoring is in place and is managed by the data center vendor. Once an attack has been identified, they will null route to traffic to stop the attack. Server monitoring systems would notify TeamCloud operations staff in the event that TeamCloud servers are experiencing latency or packet loss.

Intrusion Detection

TeamCloud's Intrusion Detection System (IDS) monitors all data center traffic into and out of customer environments. IDS alerts feed into the ticketing system and are monitored by our Vendors and TeamCloud Operations.

Data Loss Prevention (DLP)

Data in TeamCloud is always protected from access against unauthenticated or unauthorized users; however, TeamCloud does not have a third-party tool or a built-in feature to monitor for the exfiltration of specific customer data.

TeamMate employee's computers are subject to scanning by DLP tools, web filtering, and emailing scanning.

IP Address Restrictions

For an additional cost, access to your TeamCloud can be restricted to select IP addresses or ranges.

Application Isolation

Application Isolation

Clients using the TeamMate Hosted Solution are each provided separate database(s) with separate user accounts and passwords to operate the hosted software. Each client is provided with their own set of TeamMate websites independent from other clients.

Servers and Virtualization

Virtualization

With the exception of some database servers, virtualization technology is used to deliver the TeamCloud environment. Direct access to the virtual machine host is severely restricted to a few select members of TeamCloud operations team.

Servers

Servers on the TeamCloud network run Microsoft windows server operating systems. Servers are hardened and all unnecessary services are removed prior to deployment. Configuration management tools are used to ensure a consistent and accurate configuration.

Remote Server Administration

All TeamCloud administrator accounts within the environment require a two-factor VPN connection to the data center network.

Data Storage

TeamCloud uses high speed SAN Storage to provide fast, efficient, and robust data storage for our database servers.

Each client will have their own database(s) logically separated from other customer data. There is no commingled data used in TeamCloud.

Data Destruction

If a client were to decide not to renew their TeamMate or TeamCloud contract, or decided to host internally, upon request, we will provide you with a backup of your TeamMate database in Microsoft SQL format. Database files will then be erased using cryptographic erasure techniques.

TeamCloud data center vendors ensures that all drives are securely erased or destroyed at the end of their life cycle.

Standard Encryption of Data at Rest

Work papers (attachments) are encrypted within the database using AES-256 (Advanced Encryption Standard).

The database username and password are encrypted using AES 256-bit (Advanced Encryption System) and saved in an XML-based connection file.

Optional Database Encryption of Data at Rest

For an additional cost, TeamCloud offers full database encryption at rest using Microsoft SQL TDE.

Data Backup

TeamCloud operations conducts regular, reliable backups to guard against data loss if something unforeseen occurs.

Backup Frequency, Retention, and Restoration

The TeamMate Hosted Software Solution includes daily backups retained for four weeks.

All Production SQL databases are backed up nightly and then transferred off-site for safe storage (in the same jurisdiction).

All backups are retained for four weeks.

Backups are validated at least once per quarter by restoring and validating the databases.

Backups are monitored and TeamCloud Backup administrators receive an email report of any issues.

Backup Encryption

All backed-up information is encrypted both in transit and in storage.

Service Availability and Disaster Recovery

Availability Monitoring and Metrics

Monitoring tools are used to confirm system logins are available via the Internet in 5 minute intervals. Failure to login to the hosted software system within an interval will generate a system notification internally to TeamMate.

All servers are monitored 24/7/365 using various third party tools including Microsoft System Center with alerts to TeamMate Hosting support engineers (excessive CPU, Low disc space, application pool failures, etc.).

Standard Disaster Recovery

All relevant components of the data center operations and the TeamMate Hosted Software Solution are configured in N+1 redundancy, allowing all primary systems to suffer failures without interrupting service to the customer. All systems are designed to provide 99.9% availability to customers using TeamCloud.

The TeamCloud does not have a warm or hot standby site. TeamMate will provide all commercially reasonable efforts to restore service. We have an agreement with Vendors that in the unlikely event of a total loss of the primary facility, they will rebuild our infrastructure to an equivalent facility. This will then be rebuilt using the previous night's offsite backups.

Disaster recovery (DR) plan is not customer specific and is tested at least once per year.

Enhanced Disaster Recovery

More extensive recovery options may be available with custom contract terms.

Business Continuity

In addition to the disaster recovery solutions mentioned above, Wolters Kluwer maintains business continuity plans and an associated business impact assessment.

Protection from Malicious Code

TeamCloud uses anti-malware tools on servers and workstations to prevent malicious software from affecting the TeamCloud environment. Anti-malware product is configured to protect in real time on all hosted servers. The anti-malware library definitions are checked for updates at least once per day.

Vulnerability and Patch Management

TeamCloud uses several third party tools (Nessus, Rapid7, etc.) to perform monthly security vulnerability and patch management scans of both our internal and externally facing systems. Our vulnerability management policy stipulates remediation timeframes for critical, high, medium, and low vulnerabilities. Critical items are to be addressed immediately.

Server patching and TeamMate hotfixes are applied outside of business hours without any disruption of service.

SIEM and Audit Logs

Infrastructure related audit logs are protected from unauthorized access, protected from modification, and retained for a period of 90 days. For privacy and security reasons, we do not allow customers to review infrastructure log files.

All other Normal Microsoft log and event viewer entries are used per Microsoft's best practices.

The TeamMate application has internal Log files that are used if required.

Segregation of Duties

Segregation of duties has been implemented in key technical operational areas of TeamCloud operations. Examples include access management and change control. Database access is restricted to a select number of TeamCloud operations staff.

TeamMate Support, Development, and Quality Assurance teams have no access to TeamCloud servers or infrastructure.

Change Management

TeamCloud change management policy governs change management practices for the TeamCloud environments. The policy includes requirements for approving changes.

Logical Access

Account Provisioning

User accounts to the hosted environment will be created and managed by TeamMate staff. User account additions, removals or reactivating of inactive accounts can only come from designated TeamMate champions. Calls to the Helpdesk are logged in our ticketing system first before being transferred to the TeamCloud Support group.

Access to the TeamMate Application will be performed by designated champions within your audit department. TeamMate user account additions, removal, and password resets within your TeamMate instance will be managed by your designated TeamMate champions or System Administrators.

Users can use the self-service feature within the application to manage and maintain their passwords 24x7.

Account and Password Policy

Access to the TeamCloud application servers is via a user account and strong password:

- Blank passwords are prohibited and will never be used.
- Passwords shall be of a minimum length of eight (8) characters and at least two of the following character types: Alphabetic, Numeric, Special Character.
- Passwords shall not be the same as the User ID.
- Users shall be required to change passwords at least once every ninety (90) days.
- Passwords shall be at least one day old before they can be changed.
- The 24 most recent passwords cannot be used when selecting a new password.
- Group, shared or generic user IDs are not created in the FULL hosting environment.
- All user accounts (administrator and user) are subject to the same password policies.
- Passwords are stored in Microsoft Active Directory.

- Microsoft Active Directory manages failed login attempts. Account lockout duration is 30 minutes. The account lockout threshold is four (4) attempts and reset account lockout counter after 30 minutes.
- Sessions are ended after a period of 1 hour inactivity.
- Inactive TeamCloud accounts are disabled after 90 days of inactivity.

TeamMate Application Passwords

Standard TeamMate password restrictions and can be configured within your TeamMate database using the following parameters:

- Password Complexity
  - Minimum number of characters 6-20
  - Minimum number of capital letters (0-5)
  - Minimum number of numeric characters (0-5)
  - Minimum number of punctuation or special characters (0-5)
  - Password cannot match login name (Y/N)
- Password Expiration:
  - Force password reset after number of days (0-365)
  - Disallow the last number of passwords to be reused (0-10)
  - Maximum number of login attempts before account is locked out (0-5)

Passwords are stored and encrypted in the TeamMate database.

TeamMate highly recommends the following:

- All vendor default passwords changed
- Requirement to not share passwords

Revalidation and Revocation

Access rights within your TeamMate Application will be the responsibility of your TeamMate champions and/or System Admins.

A monthly access review and revalidation of administrative access rights to the TeamCloud environment (TeamMate Employees) is performed and revokes access when it is no longer required. **We also highly recommend that our customers do the same for their environment.**

Wolters Kluwer Human Resources team notifies TeamCloud operations when a Wolters Kluwer employee or contingent worker is terminated or changes from one department within the company to another. The individual's access is then revoked or modified.

Our data center vendors perform similar reviews.

SSO or Federated Identities

We are currently unable to interface with clients Active Directory or single sign on systems (SSO).

Physical Security

Access Control and Access Revalidation

All Wolters Kluwer offices and third party data centers have implemented access controls to prevent access by unauthorized persons. TeamCloud's data center vendors use a combination of biometric and keycard access. Data centers have 24x7x365 security personnel.

Visitors

Visitors to Wolters Kluwer offices must sign and register. Visitors to our vendor data centers must be pre-approved by TeamMate and the vendor. Once at the data center, visitors must show government issued identification and sign in. All visitors receive a visitor badge and will be escorted at all times. No access will be provided to the server room(s).

Surveillance Cameras and Monitoring

All third party data centers have surveillance cameras covering ingress and egress locations with 24x7x365 security monitoring.

Personnel Security

Background Checks

All Wolters Kluwer employees undergo the following checks where allowed by law:

- Criminal
- Verifications of employment
- Education
- Social Security trace search (or international equivalent)

Training and Awareness

Wolters Kluwer provides mandatory information security training and awareness to all TeamMate employees and contingent workers.

TeamMate provides several methods of security training for developers.

Termination and Collection of Assets

Upon termination of an employee or contingent worker, Wolters Kluwer HR Team will notify TeamCloud Security Team and any Wolters Kluwer assets assigned to the employee will be collected.

Employees of Third Party Data Centers

All staff of off our third party data centers are employees of the data center and undergo pre-employment screening.

Security Program, Risk Assessment, and Policies

Security Program Management

TeamCloud operations team hold industry security certifications such as the CISSP, CCSP, CISM, and CEH along with Microsoft, Cisco, and VMware certifications.

In order to ensure that Wolters Kluwer management team and various organizations participate in the security program, the Wolters Kluwer Security Committee is comprised of individuals across the company and meets at least once per month.

Security Policies

Wolters Kluwer has implemented a full suite of security policies that are reviewed at least once per year by the Security Team and are approved by the TeamMate Security Committee. Employees are trained on the policies upon hire and are required to attest to reviewing the Security Policy and the company code of conduct once per year.

Security Incident Management

TeamCloud's Incident Response Policy and process ensure that all incidents are managed, that management personnel are involved, and that appropriate communications occur. Customers are notified of a confirmed security breach within 48 hours via email. All security incidents are managed by Wolters Kluwer's Security Team and have contracted with expert third party security investigative resources to be available in the event their services are required. Wolters Kluwer will involve law enforcement when necessary.

Third Party Audits or Assessments

TeamCloud uses third party audits and assessments to both help identify issues with our security controls and to help assure our customers of those controls. TeamMate participates in a large number of third party audits or assessments and each one is described below.

SOC2

TeamCloud current SOC2 report covers the period October 1, 2015, to September 30, 2016 and is available under NDA. Please contact your sales representative to request a copy.

Copies of our data center vendors SSAE16 / ISAE 3402 Type II SOC 2 reports are available upon request. They are issued along with a confidentiality statement that must be accepted by the customer receiving the report and cannot be re-distributed. Please contact your sales representative to request a copy.

ISO 27001

All of our data center vendors are required to hold and maintain the International Organization for Standardization (ISO) standard 27001, version 2013. This certification provides our customers with an extra level of assurance regarding the maturity of over data center vendor's security program and security related controls.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

HIPAA establishes a set of safeguards for receiving, transmitting, and maintaining the security and privacy of healthcare data for healthcare providers and their business associates.

TeamMate will sign Business Associate Agreements ("BAA") with clients. Please contact your sales representatives for more information and costs.

Software Development

This section describes several key security controls in TeamMate development environment. Security is embedded into the TeamMate Software Development Lifecycle (SDLC). TeamMate follows a secure development life-cycle (SDL) modeled after Microsoft's recommended SDL.

Design Phase

During the design phase for new products or major features, the security team assists with identifying security risks and requirements.

Development Phase

During the development phase, the development team incorporates the requirements identified in the design phase. This ensures the proper security controls are addressed in the development cycle. Developers use secure coding practices to reduce potential security risks.

Source Code Reviews

Code reviews are a mandatory, perpetual process in TeamMate's development lifecycle. Each commit must undergo a peer review.

This includes security as part of the development process from training the entire staff on security, to considering security during design and architecture, all the way through release and includes a response process.

During the verification phase, we have a third party review our security process in hosting (see SOC 2 audit) and perform dynamic scanning using IBM App Scan. These tools focus on confirming use of best practices such as the OWASP Top 10 and other industry recognized security practices.

Quality Assurance Testing

TeamMate QA process requires security testing as part of the testing and quality assurance process. This process is designed to test the new security controls as well as the previous security tests. Tests also check for any security vulnerabilities identified in previous releases.

Development and Hosting Isolation

TeamCloud production, development, and QA environments are separated both logically and physically. Customer data is not permitted to be in the development or QA environments without express permission from the customer and a mutually agreed upon sanitation procedure.

Third Party Security Testing

The TeamMate Hosted solution is tested yearly by an independent third party for both infrastructure and application vulnerabilities. The TeamCloud Security and Development teams reviews the resulting report and follows up on each of the findings.

TeamCloud infrastructure is constantly monitored for vulnerabilities using commercial Vulnerability Assessment Solutions.

The TeamMate applications are tested for vulnerabilities during all stages of the quality assurance and testing processes.

Scheduled Maintenance and Upgrades

TeamMate Upgrades

A minimum twenty one (21) days' notice will be given for scheduled maintenance and upgrades that will require user downtime. Advance notice will be sent to TeamMate Champions via email.

All upgrades to the TeamMate Software Suite are performed by TeamCloud operations staff, there is no user or user IT involvement required.

As the hosting environment is a shared resource, all clients are upgraded at the same time.

Scheduled Maintenance

TeamCloud does not have fixed scheduled maintenance windows. A minimum twenty-one days' notice will be given for scheduled maintenance that will involve user downtime. Notice will be sent to registered TeamMate Champions via email as well as notification on TeamCloud login pages.

Emergency Maintenance

We try to schedule any maintenance that may affect user access but under certain circumstances, we reserve the right to do emergency maintenance.

Server patching and TeamMate hotfixes

These are applied outside of business hours without any disruption of service.

Platform Support

Detailed information about supported platforms is contained in the *TeamMate AM IT Overview*, which is available on TeamMate Connect.

> **NOTE**: With TeamMate version R12 we have added support for Chrome and Edge browsers.

> **IMPORTANT**: Access to the TeamCloud portal to run the desktop apps (EWP, TeamAdmin, etc.) will still require Internet Explorer. Chrome and Edge are not supported to access the TeamCloud Portal. TeamMate websites, TeamCentral, TEC, etc. will work with IE11, Chrome and Edge.

Desktop Requirements

There are no additional software requirements unless you are planning to use the limited use offline TeamEWP feature (see limited use offline feature below)

As TeamCloud is always at the latest TeamMate version, please refer to the latest TeamMate Suite IT Overview Document for supported PC hardware configuration, operating systems and latest web browser support.

NOTE: “Office version” or the “other requirements” are not necessary.

Limited Use Offline Feature

TeamCloud is designed to be a SaaS solution that requires as little maintenance on the client end as possible, but we do understand that there may be *occasional* or *emergency* situations when you need to access TeamMate but do not have a connection to the internet.

TeamCloud will allow you to use the TeamEWP replication feature to copy a replica locally to work on while you are not connected to the internet. Users who wish to use this feature will need to install the TeamEWP client locally.

NOTE: If you are planning to use the Limited Use TeamCloud offline feature then:

The client computers must meet the minimum requirements set out in the most current TeamMate IT Overview document.

It will be the responsibility of the client to initially install this software and upgrade it every time the TeamCloud system is upgraded. **Remembering that TeamCloud is regularly patched with the latest versions of TeamMate.**

Latest Downloads will be available on TeamMate Connect.

Creation of a replica should be done at a location with a good connection to the internet. The speed of creation and transfer of the replica will depend on the amount of available bandwidth and latency. The actual creation times will depend on the size of the replica being created and the available bandwidth available at the time of the transfer. The larger the available bandwidth the faster the files will transfer.

As with all major TeamMate upgrades replicas that are not merged before the upgrade will be discarded.

Bandwidth Requirements

TeamMate AM require an average of 100 Kbits per second (Kbps) with Latency less than 100 milliseconds per user. Anything above this and you will start experiencing lag in the TeamCloud session.

TeamCloud does not use a constant amount of bandwidth; it actually tries to reduce bandwidth usage to zero when nothing is changing on the screen. Bandwidth consumption only goes up in proportion to what is changing on screen.

Upload and download speeds (attaching and exporting workpapers) will also depend on the amount of available bandwidth and latency. The actual upload times will depend on the size of the file being transferred and the available bandwidth available at the time of the transfer. The larger the available bandwidth the faster the files will transfer. Typical upload speed when attaching documents in EWP using TeamCloud are 0.10 – 0.50 MB/sec.

To help in determining your internet speed and latency to our data centers you can use the following utility at https://speedtest.teammatehosting.com. Please not that this is to be used as a guide only and you may need to consult with your own internal IT support for more information.

Additional Questions

For additional information or inquiries, please contact your TeamMate representative.