ADDITIVE
SOFT- & HARDWARE FÜR TECHNIK & WISSENSCHAFT

Minitab Engage™

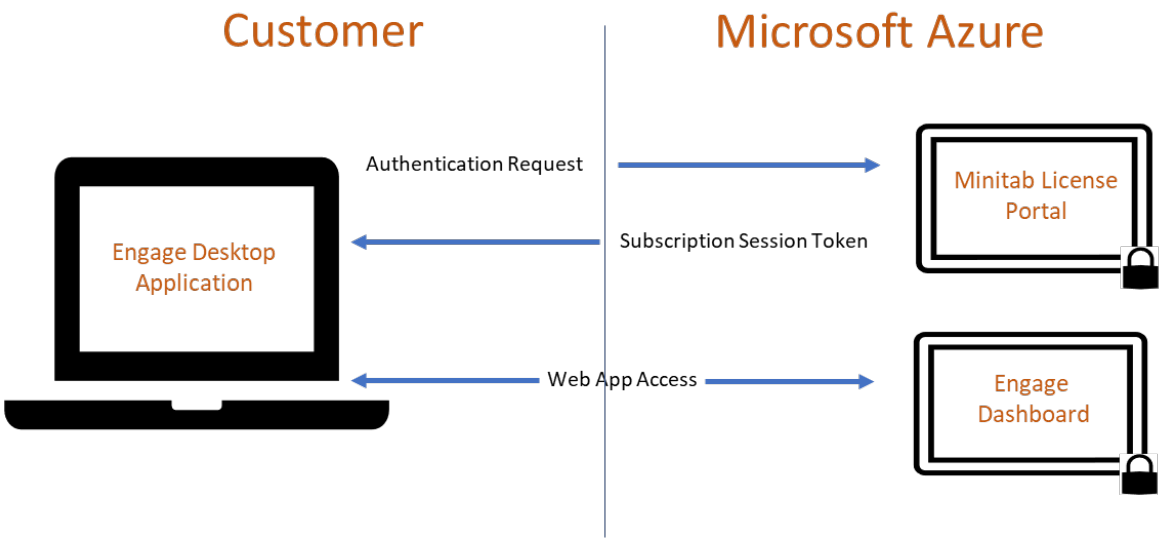
ARCHITECTURE AND SECURITY

REVISION DATE: 3/22/2021

Minitab®

PRODUCT AND ARCHITECTURE OVERVIEW

Minitab Engage™ is a platform for initiating, tracking, managing, and sharing innovation and improvement initiatives from idea generation through execution. Project owners and practitioners use the desktop app to execute projects. Their project information automatically rolls up to the web-based dashboard, where executives and stakeholders can view graphical summaries and reports for a high-level view of the organization's quality initiative.



The cloud optimized Engage platform consists of three components, each serving a unique purpose:

engage.minitab.com

The web application, at the heart of the Minitab Engage platform, fulfills two roles.

- Configurable dashboard display that extracts and compiles data from the Engage desktop project files to provide graphical summaries and reports for a detailed view of your entire quality initiative.
- Centralized storage for all Engage projects and templates.

Minitab Engage™ Desktop Application

The configurable desktop application, which accesses the internet to connect to the web application, provides the tools projects owners and practitioners use to execute projects.

Minitab License Portal

This company-wide Secure Token Service (STS) incorporates licensing controls, subscription management, quotas, etc. and is built on industry standard identity services.

SOFTWARE SECURITY

SHARED RESPONSIBILITY MODEL

Engage utilizes a “Shared Responsibility Model” for security. In this model, the security of the application and data is shared between Microsoft Azure, Minitab, and our customers; each playing an important role. Microsoft maintains physical security, operating system security, disaster recovery, data center physical security, and similar functions.

Minitab is responsible for configuring the system, deploying web application updates, maintaining application security, encrypting data in transit, and backing up customer data.

After the system is set up, customers are responsible for provisioning users, controlling access to the Engage application, deciding who contributes to your initiative, and deploying the desktop application (and updates).

	Microsoft Azure	Minitab	Customer
Physical and Network Security	☑		
Uptime, Resiliency and Redundancy	☑	☑	
Disaster Recovery	☑	☑	
Free Technical Support		☑	
Application Updates		☑	
Initial Setup and Configuration		☑	☑
Ongoing Dashboard Management			☑
User Account Provisioning and Access Management			☑
Project Creation and Data Entry			☑

SECURE SOFTWARE DEVELOPMENT PRACTICES

Security is an integral part of the Minitab Software Development Lifecyle. During each phase of development, security measures are in place to identify and manage potential vulnerabilities throughout development and release. These include, but are not limited to:

- OWASP Top 10 Vulnerabilities
- Security and Privacy Risk Assessments
- Threat Modeling
- Static and Dynamic Code Analysis
- Third-Party Penetration Testing

For more information on Software Development practices at Minitab, please see the Minitab Quality Statement. It includes a description of our Quality Policy, Mission, Software Development Life Cycle, and other business processes.

For information as it relates to the secure development of Microsoft Azure, please see Microsoft Azure Secure Development Lifecycle at:
https://www.microsoft.com/en-us/sdl

USER AUTHENTICATION

User accounts are established in the Minitab License Portal by your organization's authorized representative(s). The following features exist to support the security of your organization's accounts:

- **Privilege Levels:** User accounts can be segregated to provide different privilege levels for individual user accounts.

- **Automatic sign out (web):** When a user signs in through a browser, the application session continues until the browser session is closed or the user signs out of the application. If the browser is closed without explicitly signing out, the application will check to see if a user is still active after 15 minutes and if not, the user will be signed out.
- **Keep me signed in (desktop):** The desktop application has a "Keep me signed in" feature that allows users to remain authenticated after closing and reopening the application. To support this feature, the desktop application encrypts the authentication token it receives when the user signs in, then saves the encrypted token to the user's hard drive. The token is encrypted using the machine crypto key, the user's Windows sign-in credentials, and a key that Minitab determines. The user must explicitly turn this feature on and has the option to turn it off.
- **Failed Logins:** After 5 failed sign-in attempts within 1 hour, the application disables accounts for 1 hour.
- **Account De-Activation:** The customer's license administrator can deactivate the user's access to the account at any time. After the account is deactivated, the local access token will expire after a maximum of 7 minutes. After the token expires, the user cannot sign into the application.

Once accounts are established, Engage offers two methods of user authentication: 1) Password-based authentication through the Minitab License Portal and 2) Authentication through a third-party identity provider (known as deferred authentication or single sign-on).

Regardless of method of authentication, users' application permission levels are managed from within the Minitab License Portal.

AUTHENTICATION WITHIN MINITAB LICENSE PORTAL

If an organization chooses to authenticate within the Minitab License Portal, users will access their Engage subscription with a unique username and password set directly by the user. Note that there are no temporary or initial-use passwords. Password strength and complexity requirements are enforced which include:

- at least 10 characters
- at least one uppercase and one lowercase letter
- at least one number
- at least one special character (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)
- may not be the same as the account's email address

The customer is responsible for any additional training beyond the existing requirements and controls.

To further secure account access, passwords are stored in an encrypted format. Users can reset their password while they are signed into the application with their current password, or they can reset their password with a one-time-use link sent via email.

DEFERRED AUTHENTICATION/SINGLE SIGN ON (DA/SSO)

Some organizations prefer to use an authentication service that provides one set of login credentials for their users to access all their applications. This is commonly referred to as deferred authentication or single sign-on. Deferred authentication with the License Portal supports identity providers with the SAML 2.0.

DATA ENCRYPTION

ENCRYPTION IN TRANSIT AND AT REST

Engage uses an SSL certificate (TLS1.2 minimum, 2048 bit key) to encrypt all customer data in transit. Data is encrypted (using RSA / AES256) for transit both to and from the customer and for any server-to-server communication necessary for the normal functioning of the application. The application uses only private asymmetric keys and prohibits the use of master symmetric keys.

Customer data is encrypted at rest by Microsoft and is FIPS 140-2 compliant. As of January 2018, encryption at rest is the default data storage state of all new customers of Minitab, LLC online solutions. Information at rest is encrypted and protected by access controls. Only authenticated users can read, modify, or delete data as specified by the permissions associated with their account.

PASSWORD ENCRYPTION

When using Minitab authentication through the Minitab Portal, passwords are one way hashed.

SECURITY LOGS AND PATCHES

Security logs capture the following events:

- User, system, or process identifier that triggered the event
- Description of event
- Date and time of event
- Authorization information associated with the event

Security logs, which are protected from modification and destruction, are reviewed at least once a week and are maintained for at least 90 days. Security patches are applied within one year. The exact timeframe depends on the severity of vulnerability and complexity of the patch.

CERTIFICATE VALIDATION

The desktop application uses the underlying Windows network infrastructure, which uses both OCSP and CRLs, to validate certificate paths. Browsers also validate certificate paths in accordance with their individual standards.

DATA LOCATION AND MANAGEMENT

DATA BACKUPS AND RECOVERY

An automated backup strategy supports all Engage users. A full snapshot of your data is taken daily. The system retains backups for the last seven days, as well as the weekly backup for each of the past four weeks. This strategy provides daily recovery options for a seven-day window and weekly recovery options for the previous month.

DATA RETENTION

In accordance with the Minitab Engage License Agreement and the Minitab data retention policies, customer project data is retained for sixty (60) days after the expiration of the Customer's license. At that point, the customer data is permanently deleted and cannot be restored.

MICROSOFT AZURE DATA CENTERS

Engage customer data is stored in US-based data centers.

The Microsoft Azure data centers meet a wide range of internationally recognized security and compliance standards. Data centers managed by Microsoft have extensive layers of protection: access approval at the facility's perimeter, at the building's perimeter, inside the building, and on the data center floor.

COMPLIANCE AND CONTROLS

COMPLIANCE AND THIRD-PARTY TESTING

Engage was developed, tested, and audited in Microsoft's Azure environment. The Microsoft Azure infrastructure meets a broad set of international and industry-specific compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1, and SOC 2. Third-party audits of Microsoft Azure, such as those done by the British Standards Institute, verify adherence to the strict security controls these standards mandate.

As part of the shared responsibility model for security, both Minitab and Microsoft also use third-party security vendors to conduct penetration tests and security audits on a periodic basis.

Upon request, Minitab can supply the following reports and certifications for Microsoft Azure:

- SOC 1 Type 2 Report
- SOC 2 Type 2 Report
- SOC 3 Report
- ISO 27001 Certification

PROCESS AND CONTROLS

Minitab has documented a detailed overview of the controls implemented for Information Security, Privacy and Compliance. This includes, but is not limited to:

- Incident response preparation, detection and analysis, containment, eradication, and recovery.
- Threat and vulnerability management
- Business continuity management
- Identity and access management
- Security training for all employees

The frameworks referenced in the development of Minitab's processes and controls include the Cloud Security Alliance's (CSA) published Cloud Control Matrix v3.0.1 and the NIST Cybersecurity Framework v1.1

In addition, Microsoft's published assessment of Azure is based on the Cloud Security Alliance's (CSA) published Cloud Control Matrix v3.0.

Please note that Engage data is controlled by our customers and processed by Minitab. Our customers and their internal policies must control what type of information is stored in project files, including any personal, confidential, or restricted data.