TAQTILE

MANIFEST SECURITY OVERVIEW

Manifest end-to-end security was designed to keep your data secure and work in the most highly secured environments and industries.

OVERVIEW

Security and privacy are a central focus for our team here at Taqtile. We are committed to protecting our customers' data and devoted to the information security and data privacy needs of our worldwide customers. As such, we have built our product, systems, and policies with industry leading and recognized technologies and standards. And we have committed to working only with suppliers that share this philosophy and approach.

SECURE HOSTING FACILITIES

Our Manifest solution is hosted in world-class Microsoft Azure data centers to ensure the highest levels of security and availability. Benefits of Microsoft hosting services include physical security and access control, environmental controls, fire detection and suppression, power redundancy and a secure network architecture. More details are available at the Microsoft Trust Center.

Customers within the U.S. government have deployed and hosted Manifest in Amazon's AWS GovCloud (US) environment, which was designed to host sensitive data, regulated workloads, and address the most stringent U.S. government security and compliance requirements.

For customers requiring a higher level of security, Manifest can be deployed on-premise, completely within the customer's infrastructure

COMPLIANCE

Taqtile uses rigorous third-party testing and auditing to provide independent validation that our software and managed services meet the level of security that our customers deserve. We use Microsoft Azure IDS for automatic detection and prevention of possible intrusions. And Intruder.io is used for automatic and systematic penetration and vulnerability testing. Any software or code that is developed or incorporated within Manifest is automatically scanned to identify potential security issues before reaching production and before it is made available to our customers. Azure Dev Ops Security Scanner is used for our code, and we use WhiteSource Bolt to scan for any vulnerabilities in any open-source code that we use.

PRIVACY

Taqtile recognizes that privacy is a fundamental expectation of our customers and a key component to secure our customers' data. Therefore, we have technical and organizational measures in place to ensure all customer data, including personally identifiable information (PII), is protected appropriately. All customer data within the Manifest solution, when hosted by Taqtile, is resident on a dedicated, secured, cloud tenant, exclusively for use by a single customer.

CREDENTIALS AND CERTIFICATIONS

Work is always ongoing at Taqtile in this area and look for announcements in the future. We are currently working with outside auditors to complete SOC 2 compliance and certification. With this certification, we will meet standardized trust principals in security, availability, processing integrity, confidentiality, and privacy.

SECURE AUTHENTICATION

Manifest supports two-factor authentication to add a layer of security to authenticating users. It also supports Azure Active Directory (Azure AD), the enterprise identity service that many companies use to manage and secure identities. Manifest also supports single sign on (SSO) for SAML and OpenID to facilitate and seure the authentication process for users.

USER ACCESS CONTROLS

All users are assigned roles which define the level of access and functionality available to them when using Manifest. These roles vary from administrating the solution, to creating work instructions, using instructions, view only capability, and the ability to connect to other users for a video chat or remote assistance.

A special security admin role exists to specifically manage users, permissions, and their access as well as monitor data logs and domain activity. The role also provides the ability to define a set of password security rules, such as length, complexity, and age, which every user will be required to follow.

ROLE	PERMISSIONS
IT Security Admin	This role is the only role that has the ability for user management: creating and deleting users, assigning roles and permissions. It also has access to data logs to evaluate tenant activity.
Admin	This role has permissions to configure tenant settings and create domain entities such as locations, asset classes, and assets. Access to job history and reporting is also enabled. Functionality is primarily accessed through the Manifest Web Application.
Author	This role primarily enables the ability to create and edit job templates as well as the ability to create and edit entities such as locations, asset classes, and assets. Typically, only workers that have been approved to create operational procedures for the organization are assigned this role.
Operator	This role enables workers to create, perform and review jobs in Manifest. Users responsible for operating jobs guided by Manifest or reporting, reviewing and resolving 'faults' are typically assigned this role.
Viewer	This role has “view only” access to view data, preview job templates on device applications, and access general reports. This role does not enable any creation or editing or deletion of templates or entities.

All roles, except IT Security Admin can use Manifest Connect.

*A full explanation of role-based permissions and limitations is available at https://experts.taqtile.com/.

CENTRAL MANAGEMENT TOOL

Manifest has a web application for configuring the solution which also acts as a central management tool for configure and enforcing the above security policies.

ENCRYPTED FILE SYSTEM

Manifest VMs are encrypted with Azure Disk Encryption for Linux for virtual machines and use the DM-Crypt feature of Linux to provide full disk encryption of the OS disk and data disks. Thus, both system files and the database as well as files created by users such as photos and videos are encrypted. The encryption keys are stored in Azure Key Vault.

ENCRYPTED TRANSMISSION AND SESSIONS

Manifest data is fully encrypted when transmitted. Access to Manifest cloud tenant is via HHTPS using Secure Sockets Layers (SSL), a protocol designed to protect against tampering. Session Initiation Protocol (SIP) and Transport Layer Security (TLS) v 1.2 or greater is used when establishing video or audio calls with Manifest Connect.

AUTOMATIC BACKUPS AND REDUNDANCY

Manifest automatically backs up the main database instance for each cloud tenant and retains a 7 day history. A redundant copy of the last 7 days is stored outside the primary geographic region (specific regions can be requested). Similarly, associated files such as photos, videos, 3D models are automatically backed up. Backups of files occur every day as well but a 30-day history of these backups are retained.

DEVICES

oManifest is used on a variety of devices ranging from head mounted displays, such as HoloLens and Magic Leap, to PCs, and iPads. Each of these devices offer varying levels of incremental security features. For example, many Windows 10 and 11 devices offer device encryption (BitLocker) and the HoloLens has “kiosk” mode which prevents users from installing games or other applications. Also, many organizations use endpoint (or mobile device) management systems that also provide a wide range of features that further expand security scenarios such as preventing the use of a Bluetooth radio or camera. Manifest was designed to support this device functionality and these scenarios.

SECURITY MEASURE	IMPACT
Wi-Fi adapters and network access switched off	Manifest is designed to work in Offline mode.
Bluetooth radios switched off	Manifest will remain fully functional.
Camera switched off	Manifest users will be unable to capture new videos or photos or live stream video during Manifest Connect, our remote assistance feature included in Manifest.