myQA StarTrack³ Web Application CyberSecurity Leaflet

The purpose of this leaflet is to provide CyberSecurity information about the myQA StarTrack³ Web Application software to IT personnel. This information will help ensure the secure and safe use of the system in clinical practice.

What is the system used for?

In radiation therapy, treatment machines such as linear accelerators deliver photon and electron beams that must be periodically checked to ensure they operate safely and accurately over time. These quality assurance (QA) checks verify that the machine output, beam quality, and beam delivery characteristics remain within expected limits before treating patients

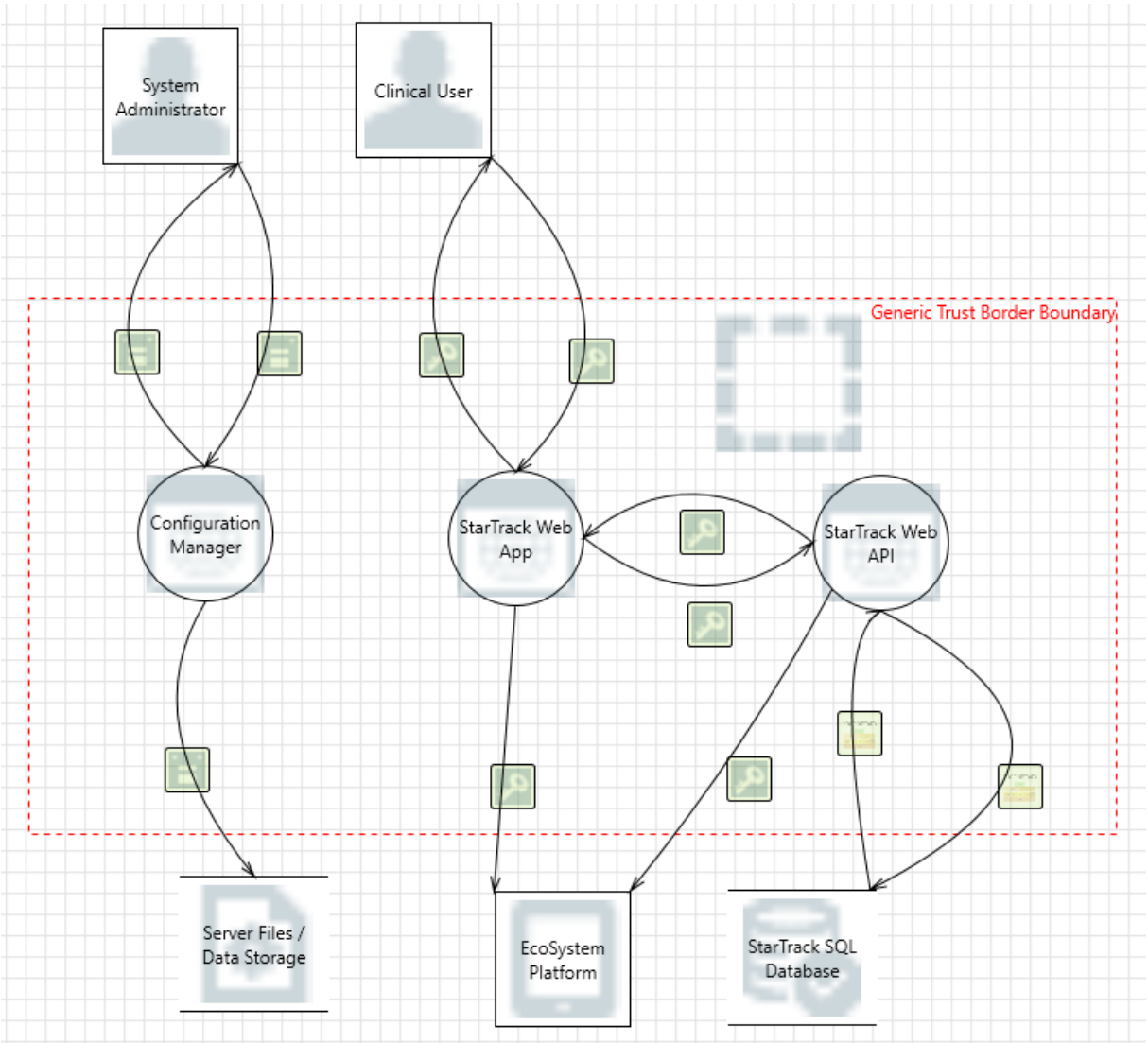
- The purpose of the myQA StarTrack³ Web Application system is to perform machine quality assurance, ensuring that radiation therapy treatment machines deliver beams correctly and consistently before patient treatments take place.
- These machine QA activities are performed by qualified medical physicists, dosimetrists, or dosimetric assistants, following clinical procedures and regulatory requirements for periodic QA of external beam treatment units.
- myQA StarTrack³ Web Application is a web-based software application that provides tools for:
    - Performing machine QA measurements, by:
        - Acquiring beam data using the myQA StarTrack³ Web Application 3 detector.
        - Applying corrections, calibrations (kTp, output calibration), and background measurements.
        - Analyzing profiles, energy parameters (e.g., TMR20/10 or R50), CAX signal, field width, and other machine-QA-related metrics.
        - Comparing new measurements with reference measurements or historical data for constancy checks.
    - Executing predefined QA tests, including:
        - Output constancy
        - Profile constancy
        - Energy validation
        - Light/radiation field coincidence tests
    - Each test automatically evaluates measurement results against expected values and displays pass/warning/fail outcomes
- Results from machine QA measurements and QA tests are evaluated within the myQA StarTrack³ Web Application WebApp. If significant deviations are detected, the physicist can determine whether recalibration, machine servicing, or corrective actions are needed before patient treatment continues.

myQA StarTrack³ Web Application CyberSecurity Leaflet

What if the measurement device fails or measured data is corrupted?

- If measurement data is corrupted or the device fails, the QA test result will be invalid and cannot be used for machine verification.
- The medical physicist will investigate the cause, repeat the measurement if needed, and determine whether the issue originates from the device, the setup, or the treatment machine.

How does the system architecture look like?



myQA StarTrack³ Web Application CyberSecurity Leaflet

Are there any operating systems or application software supplied?

- The myQA StarTrack³ Web Application WebApp software package runs on hardware provided by the operator, typically a clinical server environment.
- The operating system must be provided and maintained by the operator's IT, and the application is deployed in a client/server setup.
- myQA StarTrack³ Web Application is a web-based software composed of a backend (.NET 10) and a web-based user interface (Angular).
- Depending on configuration, the myQA StarTrack³ Web Application software package includes the following SOUPs and third-party software components:
    - Microsoft SQL Server, used to store application data, measurement data, QA test data, configuration, and audit logs.
    - OpenIddict, providing secure authentication and authorization via OIDC.
    - SignalR, enabling real-time communication for device status and live measurement updates.
- Minimum System and IT-Network Requirements:
    - Windows 11 (64-bit) is supported and recommended for server and client systems.
    - A modern web browser is required (Microsoft Edge, Google Chrome, or Mozilla Firefox).
    - Microsoft SQL Server must be available for storing configuration, measurement data, QA data, and audit logs.
    - Windows Defender Firewall, or an equivalent enterprise firewall solution, must be active and properly configured.
    - TLS 1.2 is supported; TLS 1.3 is recommended for secure communication.
    - TCP/IP must be enabled as the transport protocol.
    - WLAN IPv4 and WLAN IPv6 are supported.
    - Wi-Fi Protected Access (WPA) is required; WPA2 may be used depending on hospital IT policy. Enterprise authentication certificates are not supported.

What kind of data is stored and handled?

- The myQA StarTrack³ Web Application WebApp software package does not store any patient-related data.
- The myQA StarTrack³ Web Application server stores the following data:
    - Software error logs.
    - Audit logs (under development).
    - Measurement data acquired from the ST3 device.
    - Quality Assurance (QA) data derived from measurements (under development), such as QA tests, tolerances, and pass/fail results.
    - Institution configuration data (measurement devices, locations).

- User account information (names, usernames, email addresses; optional phone numbers)
  - It is recommended that the user removes all unused user accounts to harden the system against cybersecurity attacks.

- The myQA StarTrack³ Web Application SQL database stores the following information:
  - Measurement datasets and raw measurement values.
  - QA test definitions and test results (pass/fail, tolerances) when enabled.
  - System configuration data (machines, detectors, locations).
  - User data required for system access (no patient data).
  - Audit log entries when this feature becomes active.
- The following data are transmitted between components:
  - Between the workstation (browser client) and the StarTrack server:
  - Measurement data for visualization and analysis.
  - QA test results and pass/fail outcomes.
  - User login and authorization data (OIDC tokens).
  - Institution configuration updates (devices, machines, locations)
- Between the StarTrack server and the ST3 measurement device:
  - Measurement requests initiated by the user.
  - Live measurement streams transmitted from the device to the server.
  - Device status information (connectivity, measurement progress). Default ports for myQA StarTrack³ Web Application:
  - 80/tcp Webconfig
  - 443/tcp Webconfig
  - 1338/tcp Hermes
- Default ports for Ecosystem:
  - 7200/tcp Webconfig
  - 7201/tcp Webconfig

Notes:

- Ports may be reconfigured according to hospital IT policy, and any unused ports may be disabled in accordance with local cybersecurity requirements.
- SQL Server communication typically uses TCP port 1433.
- All listed ports use TCP and may be restricted or opened according to hospital IT firewall policy.

myQA StarTrack³ Web Application CyberSecurity Leaflet

Interfaces

- OpenID Connect (OIDC) interface, used for secure user authentication and authorization between the myQA StarTrack³ Web Application WebApp and the IBA Ecosystem identity service.
- File import interface for QA measurement files (water phantom and IC Profiler data).
- It is recommended to secure the connection between the myQA StarTrack³ Web Application WebApp and the hosting server/database using HTTPS/TLS 1.3 or newer, or by operating within a secured clinical network environment (e.g., VPN, firewall protection).

Which measures are implemented by IBA Dosimetry to support safe and secure operation?

- An MDS-2 form is published for the myQA StarTrack³ Web Application WebApp and the IBA Ecosystem and is available from our customer support team.
- Our source code is continuously scanned for vulnerabilities, and code quality is regularly assessed during development.
- Software updates are signed and protected with a SHA-256 checksum, enabling users to verify the authenticity and integrity of the update files.
- Access to the SQL database requires authenticated credentials.
    - Users who access the database from outside of the application software (SQL users) should not have a higher level of privileges than when accessing the database from within the application.
- Database Authentication Security Notice
    - For cybersecurity reasons, the StartTrack3 Web Application must not use Windows Authentication to connect to the database, particularly when the application runs under Local System or other system-level accounts.
    - Using Windows Authentication in such configurations can introduce security risks, including excessive privileges, reduced traceability, and potential privilege escalation if the host system is compromised.
    - Customers are therefore strongly advised to configure the database connection using a dedicated database account with restricted permissions, following the principle of least privilege.
    - The use of machine accounts or Local System identities as database access accounts is not recommended and should be avoided
- User authentication requires strong passwords, and login is secured using OpenID Connect (OIDC).
- Configuration files are integrity-checked at startup; if a mismatch is detected, the software switches to non-clinical mode.
- Audit logging is implemented for user-related operations and stored securely in the database.
- Communication between workstation and server uses mandatory TLS encryption.
- Only qualified personnel should have administrative privileges for server and system management.

- A secure IT environment with firewalls, antivirus protection, and controlled access is expected.
- All SOUP components are evaluated for functionality and reviewed for potential risks.
- All OWASP Top 10 considerations have been taken into account during design and testing.

Which CyberSecurity measures are expected to be implemented by the operator (health care provider)?

- The system shall be operated in a clinical and protected IT environment that maintains state-of-the-art network security standards.
- • It is recommended to assign one separate Windows account per user and to configure operating-system session timeouts according to hospital security policy.
- • User actions should be captured in logfiles and reviewed regularly to detect potential anomalies.
- General requirements expected:
    - Deploy and maintain up-to-date antivirus software and firewalls on all servers and PCs.
    - Perform prescribed maintenance and apply OS/application security patches per local IT policy.
    - Avoid using operating systems, browsers, or software versions that have reached end-of-support.
    - Configure Windows session timeout/lock for web applications according to local policy.
    - The application does not enforce automatic logout; therefore, the operating system must enforce session timeout according to hospital policy.
    - Enforce physical/electronic access control and a strong password policy for systems and network access points.
    - Do not expose the StarTrack server directly to the internet; secure internet access via the hospital perimeter.
    - Make regular backups of the SQL database and configuration, especially prior to updates.
    - To ensure confidentiality of audit logs, SQL Transparent Data Encryption (TDE) is recommended.
    - Monitor application/audit logs for anomalies as part of routine operations.
    - If wireless is used, protect Wi-Fi with WPA2.
    - Use secure browser access (HTTPS/TLS 1.2/1.3) and, where applicable, a VPN or HTTPS proxy.
    - Include StarTrack in the organization’s cybersecurity risk management and reassess after IT environment changes.
    - In order to ensure confidentiality of audit logs, it is recommended to encrypt them by using MS SQL Transparent Data Encryption (TDE).
- myQA StarTrack³ Web Application / Ecosystem specific:
    - Use TLS for client/server (web) and server/database communications; install a trusted certificate on the StarTrack server.
    - Apply IBA software updates promptly to maintain security posture.
    - Restrict administrative privileges to qualified personnel only

- Webconfig Interface
  - Restrict administrative privileges to qualified personnel only
  - Access Methods:
    - LAN (Ethernet):
      - via URL http://StarTrack-<serial>.local/ (replace <serial> with the device serial number).
      - http://169.254.22.11/ (valid if the device is connected to the PC with a direct cable connection or if no DHCP server exists on the local network).
    - WLAN (Wireless):
      - **TLS:** TLS 1.2 or newer is required; TLS 1.3 is recommended for secure communication.
      - **Wireless operation:** Supports IEEE-802.11 WLAN; the Webconfig interface provides the Wireless IP address and MAC address.
      - **Wired operation (optional):** Supports 10/100/1000 Mbit Ethernet (IEEE-802.3); the Webconfig interface provides the Ethernet IP address and MAC address.
      - **Addressing:** If no DHCP server is available, the device assigns itself a link-local address in the 169.254.xx.yy range (subnet mask 255.255.0.0). The first address to try is 169.254.22.11.
      - **SQL Server connectivity**: Ensure that the TCP/IP protocol is enabled for the SQL Server instance so the StarTrack WebApp can access the database.
      - **WLAN support:** WLAN IPv4 and IPv6 are supported.
      - **Wi-Fi security:** WPA2 must be used for wireless communication.
  - Physical Config Button:
    - Short press (< 1 s): enables the “webconfig” interface for device configuration and firmware updates. The webserver is not active (listening on ports) unless this physical button is pressed.
    - Long press (about 10 s): resets to the default network settings.
  - Related to setting up a Network Connection:
    - TLS 1.2 or higher, TLS 1.3 is recommended.
    - WLAN IPv4 and WLAN IPv6 are supported.
    - The TCP/IP protocol shall be enabled for the SQL Express Server to access the database.

- Network communication details:
  - Used in wireless mode (standard operations) - StarTrack provides wireless networking according to IEEE-802.11 for standard operations.
  - The “webconfig” interface (Device info tab) provide the Wireless IP Adress, and the Wireless MAC Address.
  - Used in wired mode (optional) - StarTrack provides 10/100/100 MBit wired networking according to IEEE-802.3.
  - The “webconfig” interface (Device info tab) provides the Ethernet IP Adress, and the Ethernet MAC Address.
  - If the device is connected to a network without a DHCP-Server, no static IP-Address is configured. A link-local address (LLADR) from the 169.254.xx.yy Pool is used (Subnet mask 255.255.0.0). The first address to try is 169.254.22.11.

⚠ Warning – Disclosures:

- Certain non-sensitive operational parameters may appear in URL query strings due to standard web communication mechanisms. This behavior is expected and does not involve sensitive or clinical data.
- The TLS configuration used by the system follows the cipher suites provided by the Windows operating system. Supported TLS versions and algorithms are determined by the host’s security configuration.
- The system generates UUID-formatted identifiers with reduced entropy as part of its standard behavior. This does not expose sensitive data and has no security impact.
- The system currently applies a permissive CORS policy. Due to the use of strict SameSite authentication cookies and non-automatic token transmission, this configuration has no security impact and will be tightened in a future update.

⚠ Caution – Physical Access Control (Operation and Storage):

- The health care provider shall ensure that the device is not kept in public spaces. Access to the premises where the device is located, shall always be controlled by appropriate technical / organizational means (e.g. using badges).

We care: what happens in the case of a CyberSecurity incident?

- IBA Dosimetry is available for you 24/7. We welcome any notification about any cybersecurity event or suspected vulnerability involving IBA hard- or software products.
- Please feel free to call our customer support team or file a request in our help center (see contact information and link below).
- We will handle such reports with high priority, and you will be continuously informed about the progress. If necessary, we will publish a security patch.

Please contact the IBA Dosimetry Support team for any further questions (helpcenter.iba-dosimetry.com):

USA, Canada, and Latin America	Europe, Middle East, Africa	Asia Pacific
Phone: +1 786 288 0369	Phone: +49 9128 607 38	Phone: +65 3129 2472
service-usa@iba-group.com	service-emea@iba-group.com	service-apac@iba-group.com