

FIRST[®] Tech Challenge Control System Network Resources (REV)

Network Infrastructure and Resource Whitelisting Guide for Schools and Facilities

Revision History	
Revision	Description
26-27.1	Initial 2026-27 Season Release

Contents

Overview	2
Control System Software Architecture	2
Hardware Management & Firmware Deployment	2
Local Device Communication	2
Network Infrastructure & Firewall Requirements	3
Protocols and Open Ports	3
SSL/TLS Decryption and Deep Packet Inspection (DPI)	3
File Extension & MIME-Type Filtering Exceptions	3
Required Network Endpoints & Whitelist Rules	4

Overview

This document provides an overview of network infrastructure configuration requirements, domain whitelisting specifications, and content filter exception rules for schools, academic institutions, and workshop facilities supporting *FIRST*® Tech Challenge (FTC) teams.

FTC teams utilize the REV Robotics Control System (including the REV Control Hub, REV Driver Hub, and REV Expansion Hub) as their core robotics platform. To configure, update, program, and maintain these devices, teams rely on host computer utilities—specifically the **REV Hardware Client (RHC)** and **REV Hardware Client 2 (RHC2)**—as well as web-based programming interfaces (OnBot Java and Blocks) served by the robot controller.

Because school networks frequently enforce aggressive content filtering, deep-packet inspection, data loss prevention (DLP), and file-type download blocks, these platforms often fail unless proper network exceptions are implemented.

Control System Software Architecture

Hardware Management & Firmware Deployment

The REV Hardware Client (RHC) and REV Hardware Client 2 (RHC2) are desktop software applications, the former running only on Windows based workstations and the latter running on Windows/macOS/Linux client workstations, with RHC2 being the preferred and longer-supported application. When an FTC device is connected to a host workstation (via USB-C or local Wi-Fi), the software:

1. Queries remote web endpoints to determine the latest approved software, firmware, and operating system versions.
2. Downloads hardware-specific binaries, APK installation packages (such as the *FTC Robot Controller* app), and system images.
3. Flashes firmware and installs software packages to connected microcontrollers and Android-based controllers.
4. Transmits application diagnostics, crash logs, and bug report forms back to support teams when requested.

Local Device Communication

In addition to remote internet access, host workstations running REV Hardware Client must be able to communicate locally with REV Control Hubs and Driver Hubs. The REV Control Hub acts as an embedded web server hosting local browser-based programming environments (OnBot Java and FTC Blocks). Students use their browser or local clients to write code, create robot hardware configurations, and export/import project files to and from their workstations. Students may also choose to use Android Studio to develop, build, and deploy more advanced applications to the REV Control Hub.

- **USB Interface:** Devices present as standard Android Debug Bridge (ADB) interfaces or virtual COM/serial ports over USB.
- **Direct Wi-Fi Interface:** The REV Control Hub creates a standalone 5 GHz 802.11 Access Point. The host PC may connect directly to this AP during programming and wireless deployment. This communication is purely local (no inbound or outbound routing through the school's LAN).

Network Infrastructure & Firewall Requirements

Protocols and Open Ports

- **Protocols:** HTTP and HTTPS.
- **TCP Ports:** Port 80 (HTTP) and Port 443 (HTTPS) must be open for all outbound connections originating from team workstations running the REV Hardware Client.
- **Local Web Interface Port:** Port 8080 (HTTP) must be permitted for local browser communication when connected directly to the Control Hub's programming interface.

SSL/TLS Decryption and Deep Packet Inspection (DPI)

Some school network appliances (e.g., Fortinet, Palo Alto Networks, Zscaler, Securlly, Lightspeed, GoGuardian) employ SSL/TLS interception and certificate re-signing.

- Automated package downloaders and command-line components within the REV Hardware Client may reject re-signed certificates that do not resolve against standard public Certificate Authorities (CAs).
- **Recommendation:** IT administrators should create an SSL/TLS Decryption Bypass / Inspection Exception rule for all endpoints listed in the Whitelist Specification Table below.

File Extension & MIME-Type Filtering Exceptions

School web filters, endpoint protection agents, and Data Loss Prevention (DLP) engines frequently block or quarantine source code files, configuration scripts, and compiled binaries.

To allow students to program robots, export project backups, and manage hardware profiles, **the network must allow the downloading and uploading of the following file types:**

File Extension	Associated MIME Types	Purpose in FTC	Common Filtering Issue
.java	text/x-java-source text/plain application/octet-stream	OnBot Java Source Code, used for programming robots.	Frequently blocked by web filters as uncompiled source code or an executable script risk.
.blk	text/plain application/json application/octet-stream	Blocks Programming Files; Proprietary XML/JSON-based block-code files.	Blocked by default-deny rules targeting unknown or non-standard file extensions.
.xml	text/xml application/xml text/plain	Robot hardware configuration profiles	Flagged or blocked by DLP policies inspecting XML data structures.
.apk / .bin	application/vnd.android.package-archive application/octet-stream	Pre-Compiled System Updates and Firmware images	Blocked under "Executable / Software Installer" file categories.

IT Configuration Note: If file extension blocks cannot be relaxed network-wide, administrators should apply an exclusion profile to the designated robotics lab IP range, device group, or student workstation Organizational Unit (OU).

Required Network Endpoints & Whitelist Rules

To ensure full functionality of the REV Hardware Client, REV Hardware Client 2, and FTC software management tools, network firewalls and proxy filters must allow outbound access to URLs matching or starting with any of the following endpoints:

Table 1: Endpoint Whitelist Specification Table

Required URL / Domain Pattern	Target Protocol	Service / Function
https://www.revrobotics.com/content/sw/*	TCP 443 (HTTPS)	REV firmware images, core software updates, and binary package storage
https://software-metadata.revrobotics.com/*	TCP 443 (HTTPS)	Official software/hardware version manifest, update manifests, and compatibility checks
https://rev-robotics-software-metadata.netlify.app/*	TCP 443 (HTTPS)	High-availability CDN/fallback mirror for version metadata feeds
https://github.com/REVrobotics/REV-Software-Binaries/*	TCP 443 (HTTPS)	Pre-compiled software binaries, USB drivers, and device utilities
https://github.com/FIRST-Tech-Challenge/FtcRobotController/*	TCP 443 (HTTPS)	Official <i>FIRST</i> Tech Challenge Robot Controller releases, APK downloads, and system dependencies
https://rhc-upload-server.uc.r.appspot.com/*	TCP 443 (HTTPS)	REV Hardware Client telemetry, error reporting, and crash log upload server (Google App Engine)
https://form.jotform.com/202376962791162	TCP 443 (HTTPS)	Built-in RHC user feedback, hardware error reporting, and technical support submission form
dl.google.com / dl-ssl.google.com	TCP 443 (HTTPS)	Primary host for Android SDK updates, platform tools, and IDE components for Android Studio
android.googleapis.com	TCP 443 (HTTPS)	Android APIs and metadata services for Android Studio
clients1.google.com / clients2.google.com	TCP 443 (HTTPS)	IDE version checks and services for Android Studio
maven.google.com	TCP 443 (HTTPS)	Google's Maven repository for the FTC SDK, Jetpack libraries, and Android X libraries, needed for Android Studio
.maven.org/	TCP 443 (HTTPS)	Maven Central repository for common Java/Kotlin libraries for Android Studio
services.gradle.org / downloads.gradle.org	TCP 443 (HTTPS)	Gradle distribution zips and wrapper downloads for Android Studio
jcenter.bintray.com/	TCP 443 (HTTPS)	Alternative artifact repository to Maven Central, commonly used by Android Studio projects

(Note: Wildcards * denote that all sub-paths, assets, and query parameters under the designated URL root must be permitted.)