The following URLs need to be whitelisted for devices to operate on the EloView 4 production environment:

EloView 4 Domains

URL	Uses
https://secure-api.eloview.com/prod	Token API / OTA updates / OS360 Warranty check - outgoing
https://secure-provisioning.eloview.com/prod	Provisioning base URL - outgoing
https://secure-broker.eloview.com	MQTT Broker URL
https://secure-logs.eloview.com	Upload logs / OTA build and private content – outgoing/incoming
https://secure-content.eloview.com	Content icons on device
https://secure-auth.eloview.com	Oauth login by device

The below URLs should also be whitelisted

https://cognito-identity.us-west-2.amazonaws.com/

https://cognito-idp.us-west-2.amazonaws.com/

https://polaris-promote-prod.s3.us-west-2.amazonaws.com

https://polaris-scan-prod.s3.us-west-2.amazonaws.com

NTP Servers (required)

*pool.ntp.org

time.android.org

Cloudfare – CDN (Content Delivery Network):

Please note: These IP's are dynamic and subject to change. It is highly recommended to whitelist by the EloView Domains provided above to avoid any disruptions in service.

104.16.64.227
104.16.61.227
104.16.62.227
104.16.63.227
104.16.60.227

2606:4700::6810:3fe3
2606:4700::6810:3ee3
2606:4700::6810:3ce3
2606:4700::6810:40e3

TeamViewer (required)

*teamviewer.com

- **Ports and URLs used by TeamViewer**

Last Modified: Jul 30, 2025

TeamViewer is designed to connect easily to remote computers without requiring special firewall configurations.

In most cases, TeamViewer will work if internet access is available. TeamViewer initiates **outbound connections** to the internet, which are typically allowed by firewalls. However, in environments with strict security policies (e.g., corporate networks), outbound connections may be restricted. In such cases, the firewall must be configured to allow TeamViewer traffic.

This article applies to all TeamViewer users.

TeamViewer ports

TeamViewer attempts to establish outbound connections using the following ports, in order of preference:

TCP/UDP port 5938

- This is the **primary port** used by TeamViewer.
- It offers the best performance and reliability.
- Your firewall should allow outbound TCP and UDP traffic to **master*.teamviewer.com** and **router*.teamviewer.com**.

TCP port 443

- Used if port 5938 is not allowed.
- Also used for:
  - Custom module deployment via the Management Console.
  - Update checks.

Note: iOS apps do not use port 443.

TCP port 80

- Used only as a **last resort** if both 5938 and 443 are unavailable.
- Slower and less reliable due to additional overhead.
- No automatic reconnection if the connection is lost.

Note: iOS and Android apps can use port 80 if necessary.

Connection behavior

TeamViewer establishes **outbound connections** from both devices involved in a session. It does **not** require any **inbound ports** to be opened on firewalls.

In TeamViewer's architecture, both devices initiate outbound connections to TeamViewer servers or directly to each other (peer-to-peer), depending on the network environment.

- No inbound ports need to be opened.
- Outbound connections should be allowed on:
  - **TCP/UDP 5938** (preferred)
  - **TCP 443** (fallback)
  - **TCP 80** (last resort)

Ports used per operating system

Operating System	TCP/UDP Port 5938	TCP Port 443	TCP Port 80
Windows	✅	✅	✅
macOS	✅	✅	✅
Linux	✅	✅	✅
ChromeOS	✅	✅	✅
iOS	✅	❌	✅
Android	✅	✅	✅

Peer-to-Peer connections

You may observe different ports being used in network monitoring tools. This is due to TeamViewer's peer-to-peer fallback mechanism, which dynamically selects available ports for communication. These are still **outbound** connections.

Destination IP Addresses

TeamViewer connects to a global network of servers. These servers use dynamic IP ranges, so a fixed list cannot be provided. However, all TeamViewer IPs resolve to: ***.teamviewer.com**

You can use this for firewall or proxy filtering if needed. From a security perspective, blocking all inbound connections and allowing outbound connections on the required ports is sufficient.

Note: If you are unable to whitelist a wildcard, please ensure the following domains are allowed on port 443:

- **configdl.teamviewer.com** – Required for downloading configuration and customization data.
- **webapi.teamviewer.com** – Required for account assignment and API-based services.

Required URLs

To ensure proper functionality of the TeamViewer interface (not needed for TeamViewer Classic), allow access to the following domains on port 443:

- **www.recaptcha.net** – Required for reCAPTCHA verification
- **www.gstatic.com** – Used alongside reCAPTCHA
- **cdn.cookielaw.org** – Required for the cookie banner

Note: If you are using TeamViewer SSO, you also need to whitelist your SSO login server.

Important
Connexion JAM
Veuillez ouvrir les connexion entrante et sortante vers :
www.jardin-de-clement.com
www.borne-jam.com
www.qrcall.shop

pour toutes pages.

ces 3 adresses sont nos serveurs JAM