T1V Network Requirements + Security

Network Requirements for ThinkHub

GENERAL

The T1V App is an application that enables wireless device sharing to T1V collaboration solutions like ThinkHub or T1V Hub. The application enables users to connect, share, and cast their device screen to the T1V room solution.

- Supports Mac OS, iOS, Windows, Android, and Linux devices
- ThinkHub and user's laptops or handheld devices can be on different subnets within your network
- For wireless screen mirroring, one ThinkHub can receive multiple connections using a single Room Identifier
- Available for free download to all T1V customers (t1v.com/app)
- T1V App connects to ThinkHub via 2 methods: Direct Mode and World Mode

DIRECT MODE

In Direct Mode, the user's laptop or handheld device must have a route on the network to talk directly to the T1V device. Additionally appropriate network policies must be configured to allow direct communication between the two devices as listed below.

- Compatible with a single subnet and/or multiple subnets
- Use Direct Mode if the T1V device and all user devices are on the same network


T1V
ThinkHub
Direct Mode
Single Subnet
Router
Network Switch
Wireless Access Point
Room ID
UUQW-CBGF
ThinkHub
A
T1V app
Mac / Windows /
Linux / iOS / Android
B
T1V app
Mac / Windows /
Linux / iOS / Android


T1V
ThinkHub
Direct Mode
Multi Subnet
Router
Network Switch
Wireless Access Point
Room ID
UUQW-CBGF
ThinkHub
A
T1V app
Mac / Windows /
Linux / iOS / Android
B
T1V app
Mac / Windows /
Linux / iOS / Android

WORLD MODE

In some situations where Direct Mode is not possible (Guest or Remote Users), typically due to the network architecture or security constraints placed on the network, T1V has developed World Mode.

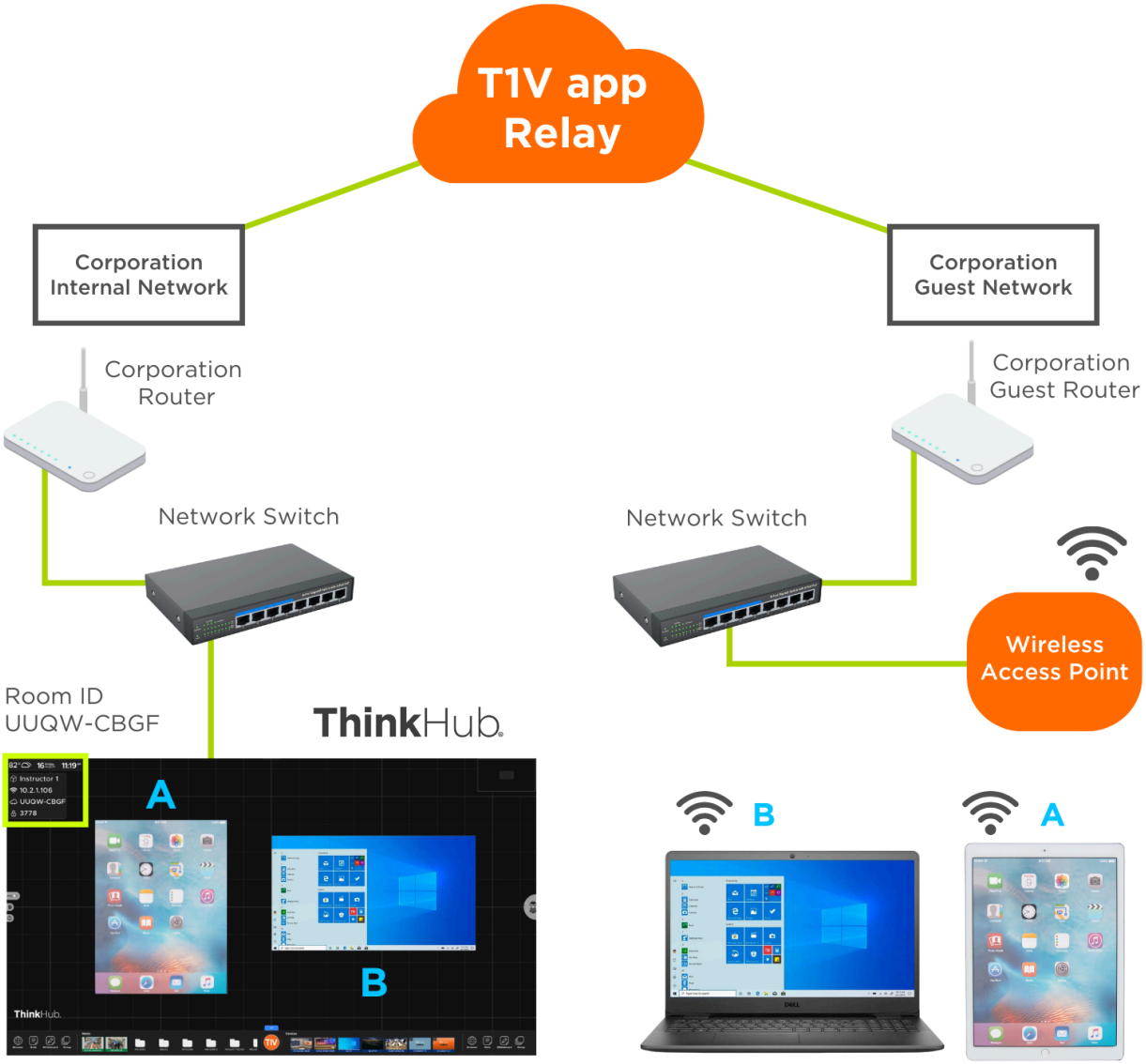
In World Mode, the device running the T1V App and ThinkHub only require outbound connections to the stream relay. All traffic to this relay is encrypted from both devices. A diagram of the architecture is shown below. The user will run the T1V App from their device and simply enter the T1V Room ID (the 8-digit code on the upper corner of the T1V display). Then, after an optional password is entered, the device will begin streaming to the ThinkHub screen.

On MacOS and Windows, if required, the application can be downloaded and executed on the fly without any installation.

Use World Mode if:

- The T1V room device is on the corporate network but you want to allow users on the corporate guest network to cast their screen to the T1V device
- T1V room device is on your internal corporate network and a laptop user wants to cast their screen from outside your network - T1V App supports this capability from anywhere in the world, even from a cellular network
- T1V room device is located on a separate isolated VLAN and employees want to cast their laptop from the corporate network (even remote users working from home)

ThinkHub World Mode



T1V APP / T1V DEVICE + PORT REQUIREMENTS

Source	Destination	Comment	Port	Protocol	Type
T1V App					
User Device	T1V Device	Direct - Control	5100, 9001	TCP	Web Socket
User Device	T1V Device	Direct - Stream data	30,000-65,000	UDP	WebRTC / RTP
T1V / User Device	AirConnectControl.t1v.com	World Mode - Control	5672 and 5671 (443 or 80 by request only)	TCP	AMQP / AMQPS
T1V / User Device	AirConnectRelay.t1v.com and 52.71.234.141	World Mode - Stream data	3478	TCP/UDP	STUN / TURN / RTP
T1V / User Device	AirConnectRelay2.t1v.com, and 34.198.94.221	World Mode - Stream data	3478 and 80	TCP/UDP	STUN / TURN / RTP

Network Requirements for Remote Support Access

GENERAL

T1V has developed several methods to allow T1V to access machines for remote maintenance. These methods have been developed to minimize the impact on a customer's internal network. In most cases simply placing your purchased T1V computer on your vendor VLAN will allow our support team to communicate with the T1V computer. No inbound port forwarding is required, nor is an external IP address required.

In some situations, a customer will decide to put the T1V computer on its own external IP address. In this situation, T1V would still require the computer to be behind a firewall to limit connection attempts from the internet. If you cannot provide this, please let your T1V sales contact or project manager know that you would like T1V to provide this.

REMOTE SUPPORT ACCESS + PORT REQUIREMENTS

Below is a list of protocols used by T1V to remotely manage machines. Ideally, T1V would like all of the below protocols supported once the computer is installed on your network.

Source	Destination	Comment	Port	Protocol	Type
TMQ – Message Queue protocol					
T1V Device	tmq-mm.t1v.com	must have a direct outbound connection, no relay or proxy	5671 (443 or 80, by request only)	TCP	AMQP / AMQPS
Log uploading					
T1V Device	s3.amazonaws.com	https://aws.amazon.com/premiumsupport/knowledge-center/s3-find-ip-address-ranges/	443	TCP	HTTPS
Screen sharing and SSH tunnel					
T1V Device	jump.t1v.com	protocol inspection turned off;this is SSH traffic over 443, not https	443	TCP	SSH

Network Requirements for Software + Security Updates

SOFTWARE UPDATES + PORT REQUIREMENTS

Source	Destination	Comment	Port	Protocol	Type
T1V Device Check-in / Content and Software updates					
T1V Device	media.t1v.com contentmedia.t1v.com t1vappsmedia.t1v.com t1vskinsmedia.t1v.com		443	TCP	HTTPS
T1V Device	cil.t1v.com		443	TCP	HTTPS
T1V Device	*.apple.com	For reference: https://support.apple.com/en-us/101555	443, 80	TCP	HTTPS / HTTP
Reporting					
T1V Device	reporting.t1v.com		443	TCP	HTTPS
Sentry					
T1V Device	35.188.42.15/32		443	TCP	HTTPS

GENERAL USE / RECOMMENDED + PORT REQUIREMENTS

The following is a list of ports and servers required for general use

Source	Destination	Comment	Port	Protocol	Type
Weather					
T1V Device	openweathermap.org		443	TCP	HTTPS
Time					
T1V Device	appropriate time server	Examples: time.apple.com, ntp.ubuntu.com	123	UDP	NTP
Touch Control					
T1V Device	Hardline Input Touch Control Module	usually on local, self-contained AV network	9003	TCP	Web Socket / HTTP
Web Browser					
T1V Device	0.0.0.0	open outbound traffic to all websites for best functionality	443	TCP	HTTPS

Web Browser - Additional Notes

ThinkHub's embedded browser does not have the ability to whitelist or blacklist websites. If whitelisting or blacklisting is required, this must be configured by the customer's IT staff using mechanisms provided by the customer. ThinkHub's embedded browser can be made to work with a proxy by request. Please submit proxy details to T1V Support to have a proxy configured, if desired.

Software VideoConferencing Integrations

ThinkHub can integrate with various software VC providers (additional costs may apply). Network requirements for these software VC providers can be found below:

- Zoom
- Microsoft Teams
- Webex
- Google Meet

Network Requirements for ThinkHub Cloud Canvas

THINKHUB CLOUD CANVAS + PORT REQUIREMENTS

The following is a list of ports and servers required for cloud canvas use within the T1V App:

Source	Destination	Comment	Port	Protocol	Type
TMQ – Message Queue protocol					
T1V / User Device	AirConnectControl.t1v.com	must have a direct outbound connection, no relay or proxy	5671 (443 or 80, by request only)	TCP	AMQPS
ThinkHub Cloud					
T1V / User Device	mpb3.t1v.com	Direct - Stream data	80 30,000-65,000	UDP	WebRTC / RTP
T1V / User Device	s3.amazonaws.com	https://aws.amazon.com/premiumsupport/knowledge-center/s3-find-ip-address-ranges/	443	TCP	HTTPS
Sentry					
User Device	35.188.42.15/32		443	TCP	HTTPS
Reporting					
User Device	reporting.t1v.com		443	TCP	HTTPS

Security: T1V App + ThinkHub MultiSite

T1V APP + MULTISITE

All T1V App and ThinkHub MultiSite data is encrypted.

When using T1V App to stream devices to ThinkHub, or when engaged in a ThinkHub MultiSite session with two or more ThinkHub devices, all data is encrypted.

T1V App Direct Mode

If you are using T1V App in Direct Mode, all data stays inside your network, and all data is encrypted.

T1V App World Mode

When using T1V App World Mode, data between an off-site device and an on-site ThinkHub is relayed through T1V's relay. In this situation, the T1V App data is encrypted with a random key that only the two endpoints know (T1V doesn't even know it). So even when it goes through the World mode relay, the world mode relay is only relaying encrypted data, and no decryption occurs in the cloud. For additional security, the random key changes multiple times throughout the exchange.

This is a feature that can be disabled as needed.

T1V App Access

T1V App Access allows users to view and control the ThinkHub Canvas from a mobile device. Both of these features can be disabled separately as needed. What's more, the ThinkHub devices houses an T1V App Access Control Panel, so in-room meeting participants can control remote user permissions.

ThinkHub MultiSite - Enterprise

ThinkHub MultiSite is an Add-On module that allows two or more ThinkHubs to communicate with one another in real time. With ThinkHub MultiSite Enterprise, all data stays inside your network between ThinkHubs, and all data is encrypted.

ThinkHub MultiSite - SMB

ThinkHub MultiSite is an Add-On module that allows two or more ThinkHubs to communicate with one another in real time. With ThinkHub MultiSite SMB, all data is encrypted from both devices. No data is ever stored on the MultiSite relay. It is only used to relay data between sites.

REMOTE SUPPORT AND ADMINISTRATION SERVICE

T1V has a remote support and administration service. This feature can be enabled and disabled by the customer as needed.

THINKHUB FILE SAVING + STORAGE

All ThinkHub canvases can be saved to a file system and have an optional password for additional protection.

OS UPDATES + SECURITY PATCHES

T1V manages all OS updates and security patches for ThinkHub/T1V Hub devices.

ThinkHub MultiSite Network Architecture

MultiSite is an add-on module distributed by T1V that provides real-time, remote collaboration sessions: anything that happens on one Canvas is mirrored to the others. Any site connected to the shared session can utilize any display configuration.

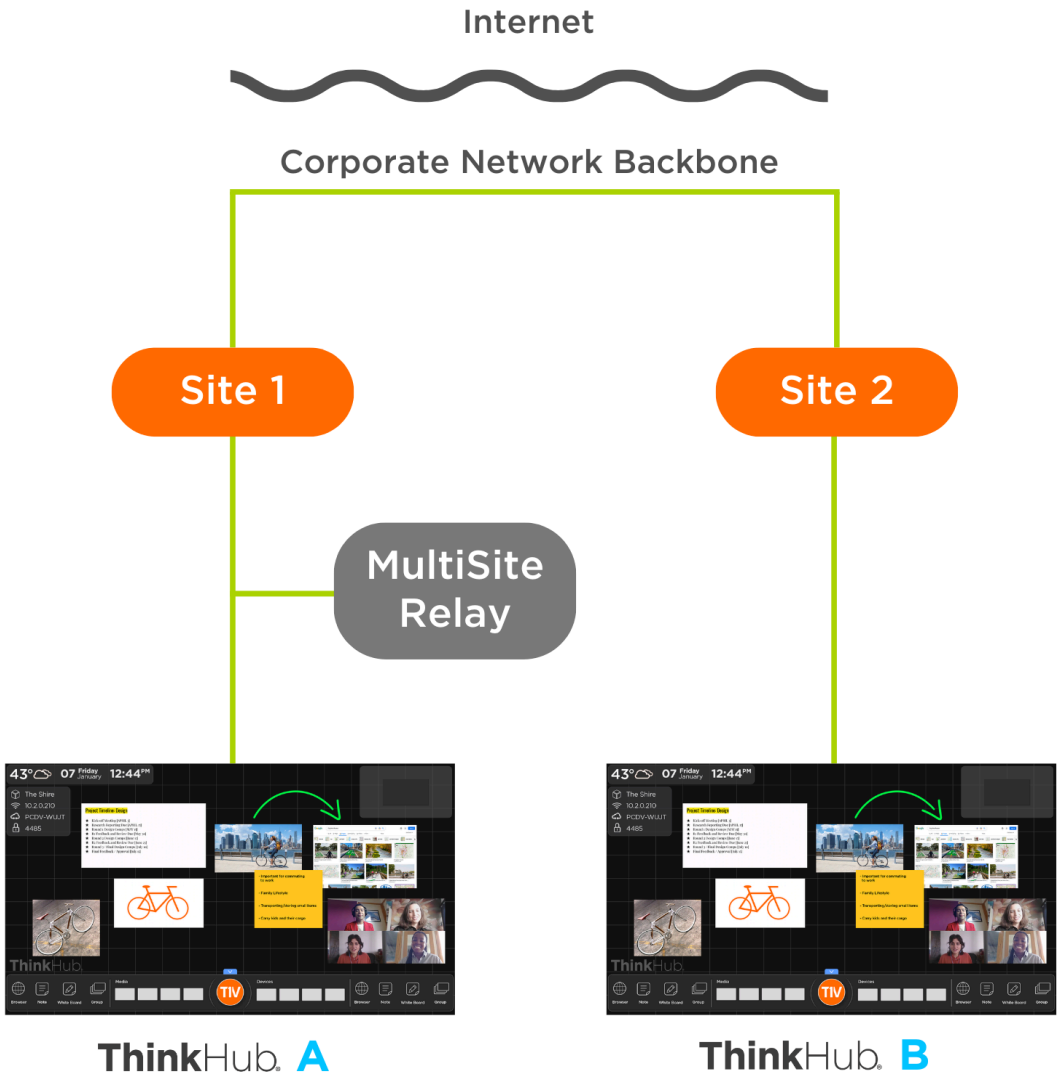
MultiSite has two options: (1) Enterprise and (2) SMB. In the Enterprise option, the connected devices must be on the same internal network which keeps all data on that network. For companies without this infrastructure between their sites, T1V has developed the SMB option.

THINKHUB MULTISITE ENTERPRISE

With MultiSite Enterprise, all ThinkHub devices and the ThinkHub MultiSite Relay are connected to the corporate backbone. This allows all ThinkHub sites to communicate with one another under the security of the corporate network. In addition, all traffic between ThinkHub devices is encrypted. No data is ever stored on the MultiSite relay.

T1V

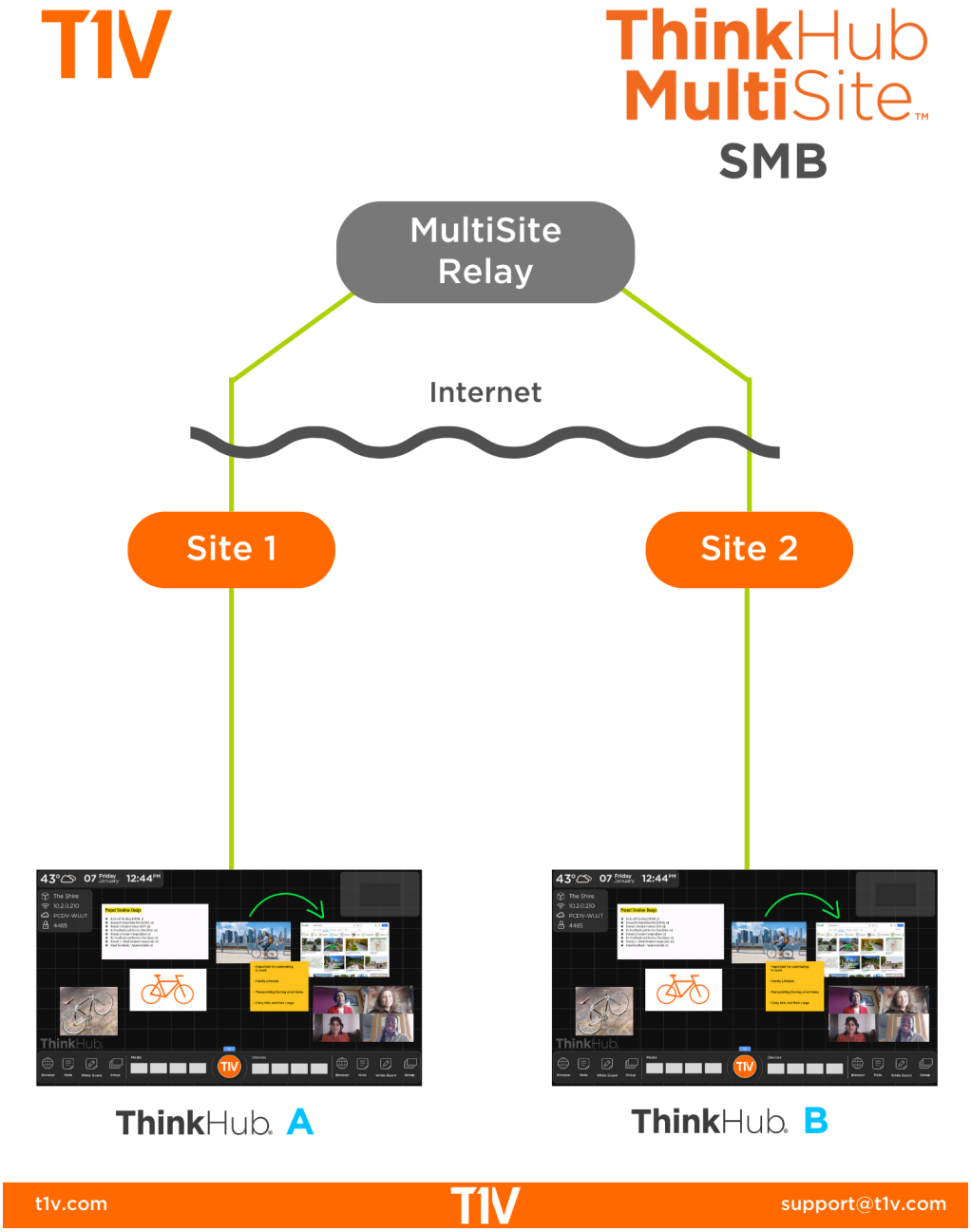
ThinkHub MultiSite™ Enterprise



t1v.com T1V support@t1v.com

THINKHUB MULTISITE SMB

In SMB, the MultiSite devices connect to each other through outbound connections to the T1V MultiSite relay. All traffic to this relay is encrypted from both devices. No data is ever stored on the MultiSite relay. It is only used to relay data between sites.



THINKHUB MULTISITE HOSTS + PORTS

Source	Destination	Comment	Port	Protocol	Type
MultiSite Enterprise / ThinkHub Education					
T1V Device	MultiSite relay (static IP)	on internal network	5672	TCP	AMQP
T1V Device	Multipoint Broadcast relay (static IP)	on internal network	8188	TCP	Web Socket
T1V Device	Multipoint Broadcast relay (static IP)	on internal network	30,000-65,000	UDP	WebRTC / RTP
T1V Device	T1V peer devices	on internal network	30,000-65,000	UDP	WebRTC / RTP
MultiSite SMB					
T1V Device	MultiSite relay (multisite.t1v.com)		5671 (443 or 80, by request only)	TCP	AMQPS
T1V Device	AirConnectRelay.t1v.com, AirConnectRelay2.t1v.com, 34.198.94.221		3478 and 80	TCP/UDP	STUN / TURN / RTP

BANDWIDTH REQUIREMENTS

This is the bandwidth required between any two ThinkHubs in a MultiSite session:
Minimum Bandwidth : 25Mb/s (both directions)
Maximum Bandwidth : 3Mb/s (both directions) x number of live streams

Note: live streams include laptops (T1V App Feeds), hardline inputs, cameras, and web browsers

ThinkHub Data Encryption

LIMITED DISTRIBUTION ONLY

T1V App (formerly AirConnect) exchanges the ip address, 4 digit pin and webRTC signaling messages with ThinkHub over a web socket (T1V App Direct - Control) that is not protected by SSL. This traffic should be protected from eavesdropping to mitigate risk of unauthorized access to ThinkHub.
All data traffic (T1V App Direct - Stream data) on T1V App and ThinkHub is encrypted. Please contact your T1V salesperson or project manager for documentation on Data Encryption. T1V monitors distribution of this material due to the sensitive nature of its contents.