

THUNDER™
Real-Time Global Collaboration Solution
System Manager Guide

Part number 370-0193-04
©2008 PolyVision Corporation
All rights reserved

Information in this document is subject to change without notice.
Reproduction in any manner without written permission of PolyVision Corporation is forbidden.

PolyVision Corporation reserves the right to make changes in product design, or detail, and to discontinue any product or material without notice.

PolyVision is a registered trademark of Steelcase, Inc. THUNDER and Virtual Flipchart are trademarks of PolyVision Corporation.
RoomWizard is a trademark of PolyVision Corporation. All other registered trademarks and trademarks used herein are the property of their respective owners.

Patents pending.

Table of Contents

Welcome	3
About This Manual	4
About THUNDER	5
THUNDER Pro and THUNDER Express	5
THUNDER System Overview	6
About the Projectors.	10
About the RoomWizard System	11
About the THUNDER Pro Wireless Keyboard	12
Planning Your Network Configuration	13
Network Security	13
Accessing THUNDER from Outside a Firewall.	21
THUNDER Pro Operating System Security	24
Application-Level Security.	26
Port Blocking Considerations	28
Installing THUNDER Express Software	33
System Requirements	33
Installing and Running THUNDER Express	33
Booting THUNDER Pro for the First Time	35
Configuring THUNDER for First Time Use	37
Entering the Serial Numbers	37
System Configuration	39
THUNDER Pro: Configure the Projectors	40
THUNDER Express: Configure the Projectors	41
THUNDER Pro: Configure the Plasma Monitor	42
THUNDER Configuration Wizards	42
Configure the Video Input	44
Configuring THUNDER Administrator Setup Pages	45
Entering and Exiting the Administrator Setup Pages	45
Configuring the Appearance of the Home Page	47
Configuring Easel Options	48
Configuring the Projectors	51
Configuring Peripheral Hardware	52
Changing the Administrator Setup Password	54
Configuring Email	55
Configuring Usage Tracking	56
Checking THUNDER Usage Status.	58
Configuring RoomWizard to Integrate with THUNDER	59
The THUNDER Client Software	60
Obtaining the Client Software	60
Installing the Client Software	61

Placing the THUNDER Client Software on Your Own Server	61
Getting Software Updates	62
Updating the THUNDER Software	62
Updating THUNDER Client Software	62
System Maintenance	63
Removing Old Sessions	63
Making Session Backups	65
Updating Windows	65
Performing Virus Checks	65
Caring for the THUNDER Pro Plasma Monitor	66
Caring for the THUNDER Pro server	66
Caring for Projectors.	66
Caring for the THUNDER Pro Stylus	70
Caring for the THUNDER Pro Wireless Keyboard	71
Diagnostics in the Room Control System	71
Troubleshooting	74
Rebooting the THUNDER Pro System	77
Appendix A: THUNDER Express Hardware Considerations	78
THUNDER Express Overview	78
Configuration Strategies	78

WELCOME

Welcome to THUNDER, the real-time global collaboration solution for sharing data and information in any format with groups and teams in any location. THUNDER is a network-enabled system that provides remote conferencing, “war room” reuse, computer desktop sharing, emailed notes, and interactive presentations.

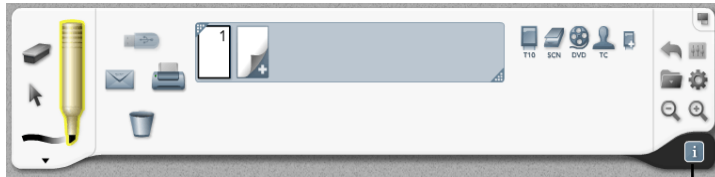


ABOUT THIS MANUAL

This manual supports the THUNDER system manager who configures and maintains THUNDER after the system is installed. The last steps in installation and the first steps in system configuration should be a collaborative effort between the system manager and A/V installer to assure that all the THUNDER components work smoothly.

This manual is one of a set of documents about THUNDER. All documents are available on-line at: www.polyvision.com. Other information that you may find useful:

- The best way to get a quick understanding of how THUNDER works is to press the “Help” button on the THUNDER easel toolbar.



Help

- *THUNDER Installation Quick Reference*: A one-page quick reference for A/V integrators who install THUNDER hardware and route cables.
- *THUNDER Hardware Installation Guide*: provides instructions for installing THUNDER hardware and routing cables.
- *THUNDER System Manager Guide*: provides instructions for IT professionals and facility managers who configure and manage THUNDER systems.
- *RoomWizard Installation Quick Reference*: provides instructions for installing the RoomWizard appliance.
- *RoomWizard System Manager Guide*: provides instructions for configuring RoomWizard.

ABOUT THUNDER

THUNDER Pro AND THUNDER EXPRESS

Two THUNDER system solutions are available:

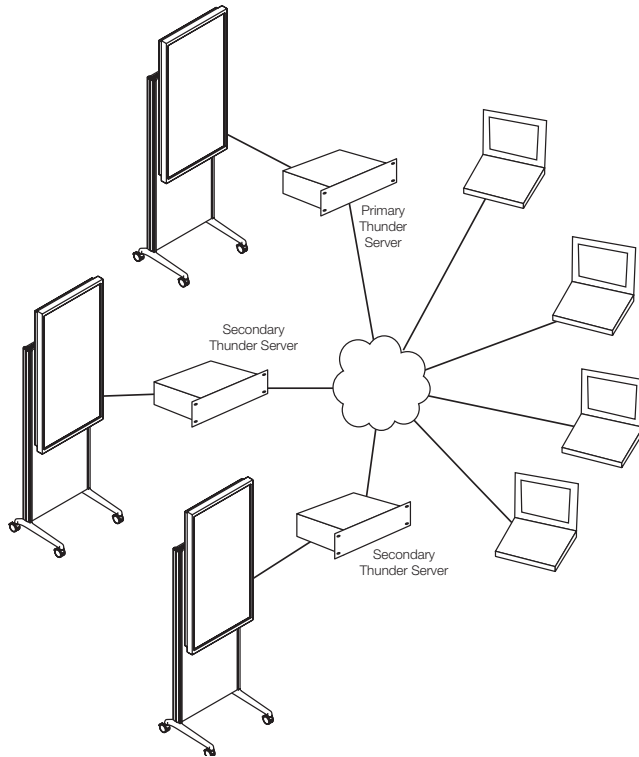
THUNDER Pro: an enterprise collaboration system with a dedicated THUNDER server, easel, and stylus for writing and sharing.

THUNDER Express: a software-only solution for Windows operating systems in which users interact with THUNDER's virtual flipchart pages using an interactive whiteboard, interactive panel, tablet PC, touch-screen plasma monitor, or other input device that is connected to a computer running THUNDER Express. For information about installing THUNDER Express, refer to "Installing THUNDER Express Software" on page 33.

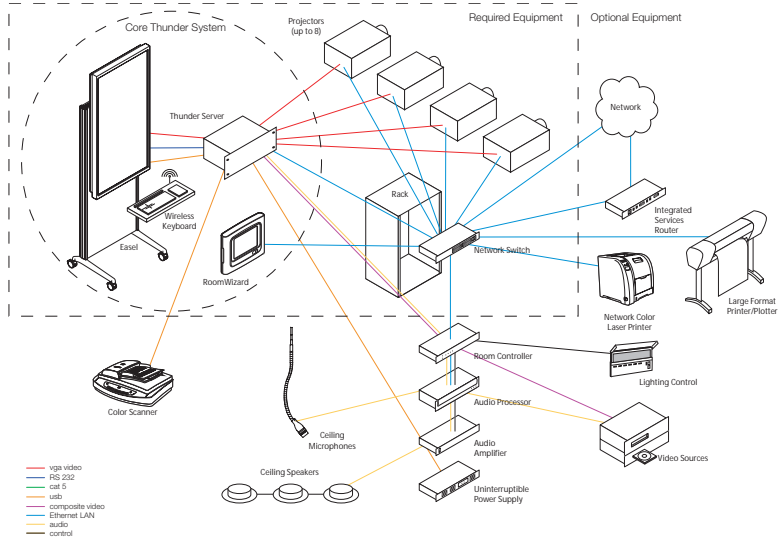
Information in this manual applies to both solutions unless otherwise specified, though THUNDER Pro systems appear in illustrations.

THUNDER SYSTEM OVERVIEW

THUNDER integrates digital media and content into a meeting, creates a stream of projected images that flow freely among groups, and enables complete creative flexibility. Following a meeting, content is seamlessly archived, emailed to all participants, and ready at the touch of an icon for immediate retrieval, whenever desired and from any location.



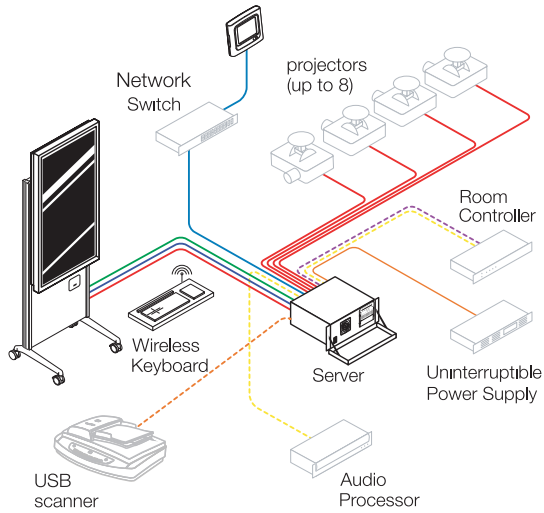
THUNDER Pro is a powerful dedicated enterprise system. The core components that Polyvision supplies with every installation are the easel (including plasma monitor and touch-screen adapter), the THUNDER server (including Windows XP as well as THUNDER software), the wireless keyboard, and RoomWizard.



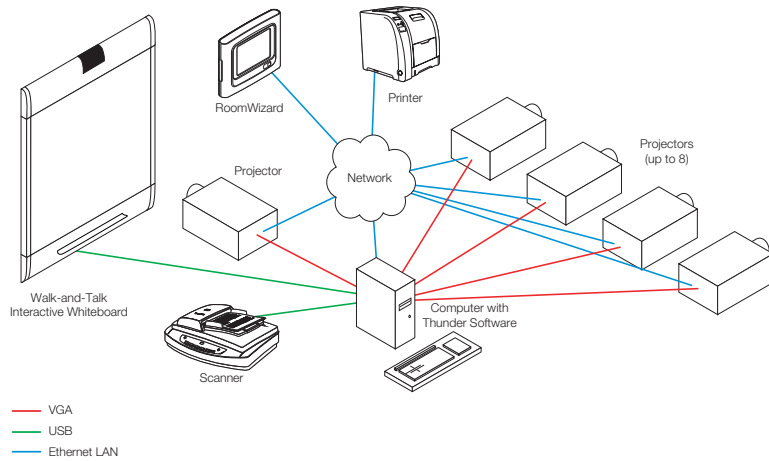
Other equipment is required for the THUNDER system, but the system designer has some flexibility in configuring components. Required components include the projectors and a network.

Equipment that maximizes THUNDER's usability include a scanner, routers, printers, plotters, video sources, lighting control, audio processor, audio amplifier, speakers, uninterruptible power supply (UPS), and microphones.

THUNDER collects and distributes information from all parts of the system. The THUNDER Pro server provides connections for the easel, scanner, projectors, amplified speakers, and video. THUNDER also connects to your LAN for, at minimum, system upgrades, backups, projector control, and integration with RoomWizard.

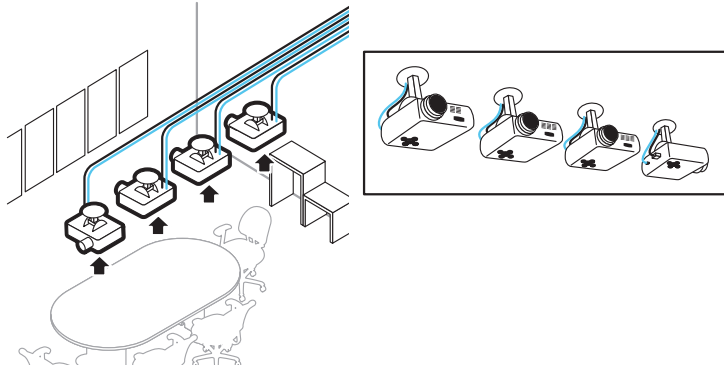


THUNDER Express is a software-only solution. It can connect to a Walk-and-Talk Interactive Whiteboard, as shown below, or many other input devices. THUNDER Express provides the same interface for collecting and distributing information from all parts of the system including the input device, a scanner, projectors, printers, video source, and RoomWizard.



ABOUT THE PROJECTORS

Projectors enable the display of flipchart pages on a wall or screen while users continue to create new pages in the virtual flipchart. Each projector can display two vertically oriented pages or one horizontal page.



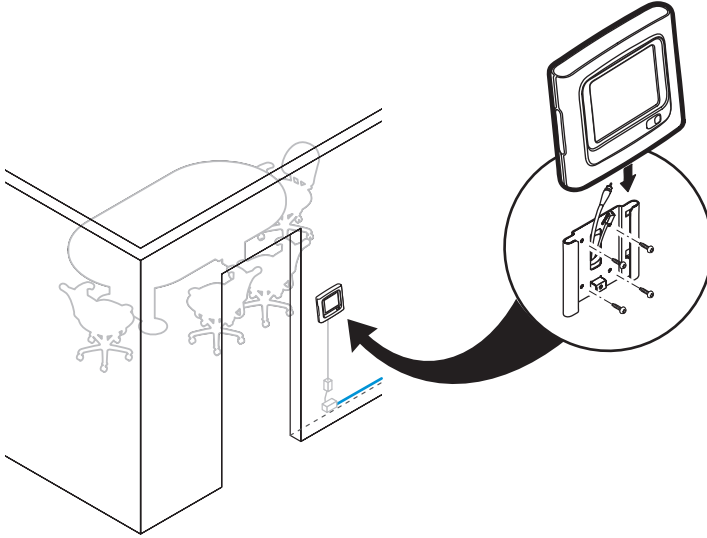
The THUNDER Pro server includes outputs for up to four XGA or better projectors. The server supports the optional addition of another video card with up to four more projector outputs.

Ethernet also connects to each projector to enable THUNDER to turn the projector on and off and to check status. THUNDER administration web pages enable you to configure the model, network IP address, resolution, and brightness for each projector. In addition, you can configure a projector for external control by a Crestron room control system. Refer to “Configuring the Projectors” on page 51.

Your license determines the number of projectors that the THUNDER system can access. If you want to upgrade to a larger number of projectors, you must obtain a new license key and reinstall the THUNDER software with that key.

ABOUT THE ROOMWIZARD SYSTEM

THUNDER integrates with RoomWizard, a self-contained web-based reservation system for meeting rooms and other shared spaces. The RoomWizard, a touch-sensitive “information appliance,” mounts outside the meeting room and connects to power and your LAN.



RoomWizard is part of your corporate network and includes its own web server. The front panel displays up-to-the-minute information about a room's schedule for that day, plus it enables users to view room schedule details and make changes in real time using the touch-screen. Refer to “Configuring RoomWizard to Integrate with THUNDER” on page 59.

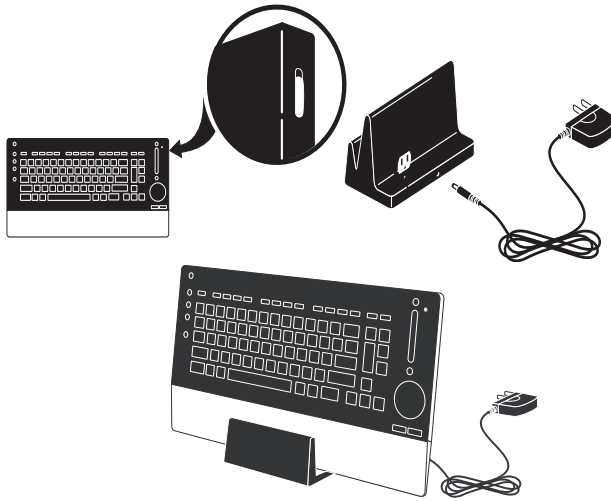
RoomWizard's One-Click Publishing feature supports THUNDER users by enabling them to email THUNDER pages to registered meeting invitees. Refer to RoomWizard documentation for details, available at: www.polyvision.com.

ABOUT THE THUNDER PRO WIRELESS KEYBOARD

The THUNDER Pro system includes a wireless keyboard. It is an essential input device for system management and also enables THUNDER Pro users to name sessions or type during the control of remote computers.

The wireless keyboard includes a convenient charging base where the keyboard should be stored for recharging when not in use.

Ensure that the charging base is always plugged in to a power outlet and the wireless keyboard is always turned on. Refer to the Refer to “Caring for the THUNDER Pro Wireless Keyboard” on page 71.



PLANNING YOUR NETWORK CONFIGURATION

THUNDER offers incredible power and ease of access for widely distributed groups of people. As with any system, that access comes with a responsibility to create a safe, secure environment for your data. THUNDER provides a number of options for configuring your system to provide the appropriate level of access and security for your organization.

NETWORK SECURITY

Network security is the first factor to consider when planning the deployment of THUNDER systems. Before purchase, you should already have a plan in place for where the THUNDER systems will sit on the network and what level of security you intend to enforce.

PLANNING YOUR DEPLOYMENT

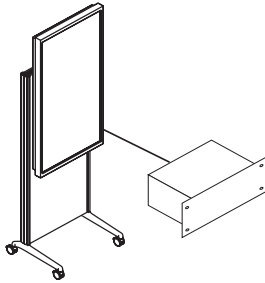
THUNDER can be deployed on your network in one of six ways:

- Standalone, as an in-room replacement for a flipchart.
- As an island, used within a very limited network space that doesn't allow outside access.
- On your internal LAN with no outside access, available to anyone in your organization with permission.
- In a demilitarized zone, providing access from inside your LAN and from the outside as well.
- On your internal LAN with outside access through the firewall, available to users both inside and outside your organization.
- Directly on the Internet, providing public access.

Each of these deployment methods are discussed in the following pages.

STANDALONE

A standalone THUNDER system is a THUNDER system which is not networked. It is the most secure installation possible, because the only way to gain access is by being in the room with the system.

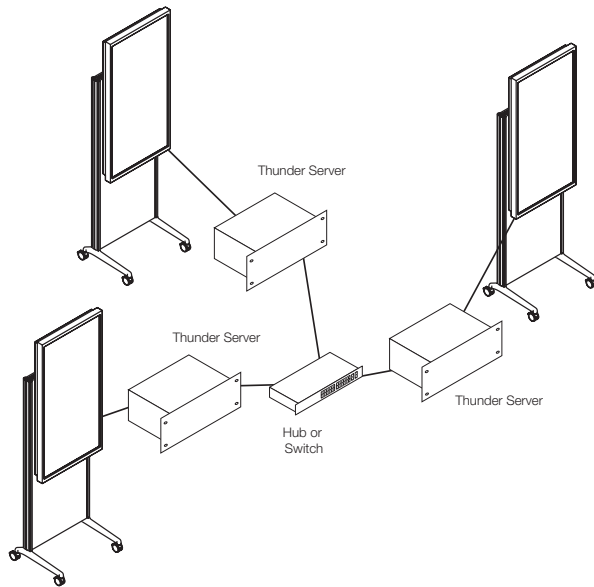


Many of the features (such as emailing notes to participants, connecting two or more systems together, and the ability to show live content from other computers) are not possible when the system is not connected to a network. However, a standalone system can be very useful:

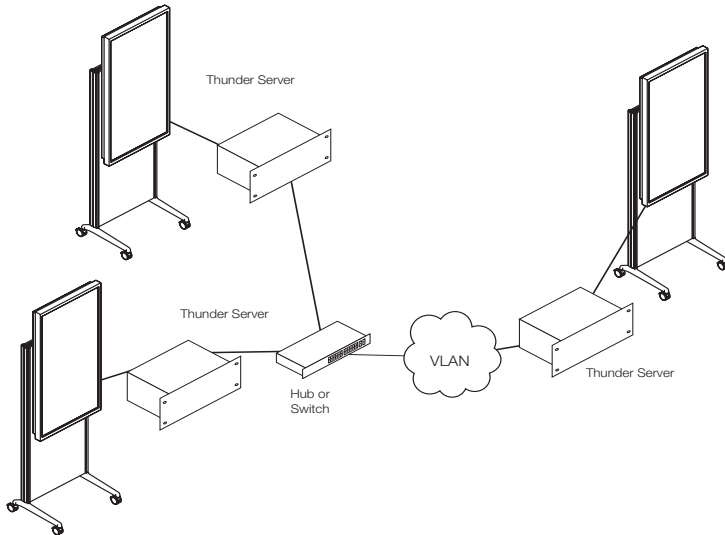
- The system can be used as a virtual flipchart, allowing electronic editing of content.
- You can save sessions and recall them later, which allows you to use the room for multiple projects throughout the day.
- You have an immense amount of storage for your ideas.
- Sessions can be printed.
- Sessions can be saved to a USB mass storage device that you connect directly to the easel.

ISLAND

An island is a network which is dedicated to a specific set of devices but not attached to the general network. For instance, a corporate training facility could be on an island. All of the devices (THUNDER systems, RoomWizards, and the wireless networking hubs) in these classrooms might be on a single network, but that network would not be connected to the outside world.



An island does not necessarily need to be located all at one site. For instance, an island might extend between two campuses and encompass only the THUNDER systems on each campus. A VLAN could be used to connect the two portions of the island together over a wide-area network.



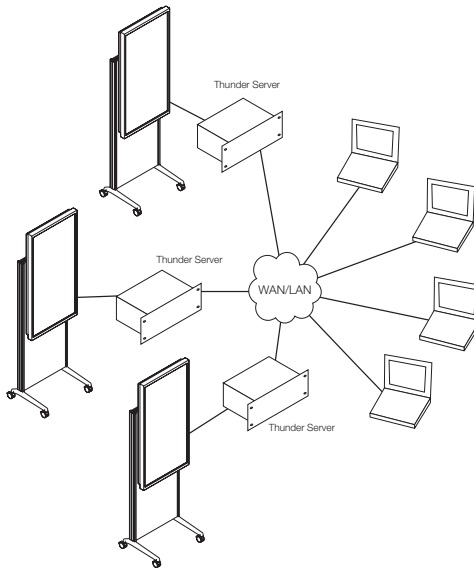
Islands are an excellent choice when remote collaboration is required, but complete privacy is also needed. Islands ensure that no data can leave the private network, thereby guaranteeing complete security. In addition to the capabilities of a standalone system mentioned above, with an island:

- You can collaborate between two sites with the utmost security.
- You can share and control screen content on a THUNDER system from any laptop in the room that is networked to the island (through wired or wireless networking).
- You can save sessions in multiple locations simultaneously and load them independently later.
- Your participants at any connected THUNDER easel (or laptop) can edit content simultaneously.
- If there is an e-mail server available on the island, sessions can be automatically e-mailed to participants during (or at the conclusion of) a meeting or class.

Islands are often used by educational institutions.

INTERNAL LAN/WAN ONLY

Many corporations choose to place THUNDER systems on the internal corporate network only, but offer no outside connection capability. This is an excellent solution for globally distributed companies because any employee can gain access to a THUNDER system to participate in meetings (if they are given the password for the conference in progress). At the same time, the system is isolated from outside hacking and viruses. The session data is kept secure within the organization.

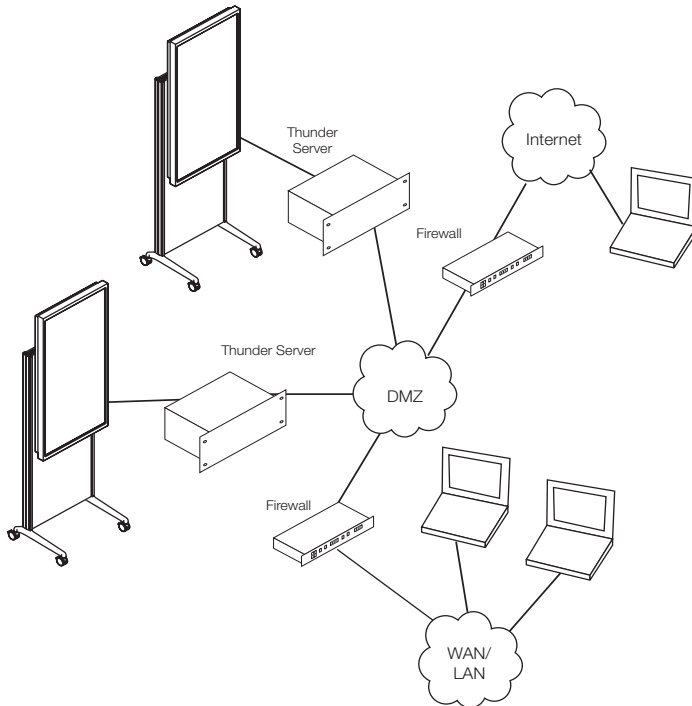


This is the most common installation of THUNDER. In addition to the capabilities of an island mentioned above, using the internal LAN provides these features:

- You can have impromptu meetings with anyone in your organization.
- Your remote participants can be located on-site or off-site through the use of Virtual Private Networking (VPN). For instance, employees or students can connect in from home or in an airport.
- Any easel can connect to any other easel(s), providing the maximum opportunity for participation.

DEMILITARIZED ZONE

Although installing a THUNDER system on an internal LAN or WAN makes the system available to all employees, there are times when it is useful to have outside participants such as vendors, contractors, and trainees gain access to THUNDER. At the same time, security of the corporate network must be preserved. The solution for this is to create a demilitarized zone (or DMZ) for THUNDER. A DMZ is a network located between two firewalls. One firewall provides port openings for access from the Internet while the other protects the corporate network from any prying eyes.



DMZs are excellent from a security standpoint because network administrators can carefully configure exactly what access is allowed to the THUNDER system without potentially exposing other more sensitive internal systems to outside prying. At the same time, users inside the protected LAN can gain access to the THUNDER server through a protected firewall. Since all hosting is done on an internal server, configuring the system for maximum security can be tightly controlled.

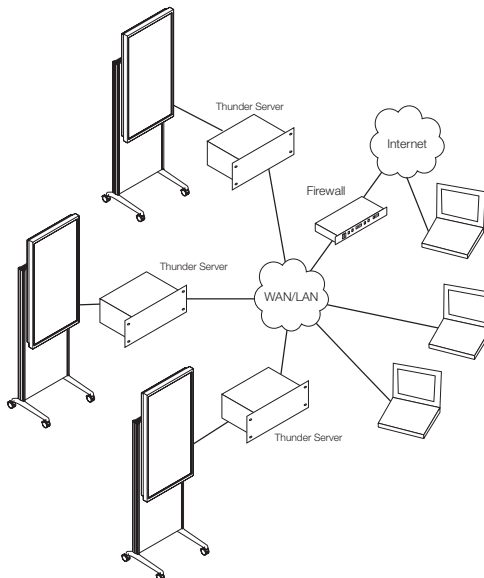
Using a DMZ adds these capabilities to the LAN/WAN configuration above:

- Any remote participant with access to the Internet can connect directly into a THUNDER session.
- You can provide training to outside people without incurring any outside service charges from THUNDER.
- Employees can hold impromptu conferences with outside customers, trainees, vendors, etc.

It is important to note that placing sensitive information on a system accessible through the Internet should be avoided, if possible. Password protected sessions and conferences at a minimum to protect sensitive communication.

INTERNAL LAN WITH OUTSIDE ACCESS

DMZs provide a secure environment for outside access. However, one downside is that they may require the THUNDER equipment to be located near the internet drop physically. An alternative is to provide direct access to a THUNDER system by opening ports to a specific IP address (that of the THUNDER system). In this way, outside access can be granted while maintaining security for the rest of the corporate network.

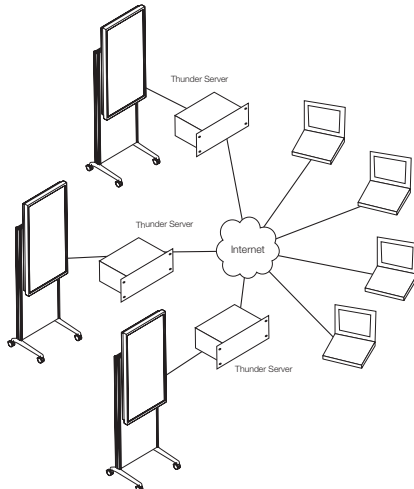


This solution can be a very cost effective way to provide outside access, but it does increase the risk of security issues. If malicious software makes its way onto the THUNDER system, the remaining systems on the network can be at risk. Therefore, it is important to provide strong virus protection on the THUNDER server and to disable all but the minimum set of ports required to operate THUNDER through the firewall.

This solution provides some convenience and cost savings over the DMZ solution, but it does not provide any additional end-user features.

PUBLIC ACCESS

There are some installations where THUNDER is to be used exclusively for public access. For example, an outside training firm, a real estate company, or a community college campus are excellent locations to use a public access THUNDER system.



This configuration places the THUNDER server directly on the Internet. THUNDER's underlying communication software was designed to provide public access to a wide range of users. As with any publicly accessible server, great care should be taken to ensure that the system is backed up at regular intervals, the operating system is updated with security patches regularly, and strong virus protection is installed.

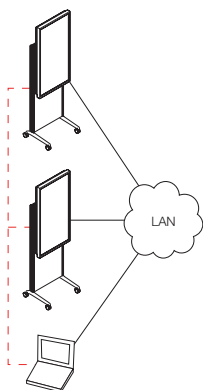
The advantage of a publicly accessible server is that no internal LAN resources are placed at risk because they are completely isolated from the THUNDER server. This solution is excellent for training large groups of widely dispersed people.

ACCESSING THUNDER FROM OUTSIDE A FIREWALL

To make remote participation work properly, the configuration of one or more firewalls must be taken into account. This section presents some specific examples of connecting THUNDER systems and clients through firewalls to help the system administrator make outside access possible.

Each section below describes a different potential scenario. Physical connections are shown with a solid black line. Logical connections are shown with a red dashed line.

THUNDER inside a Firewall or through VPN:



On a local area network (LAN) or wide area network (WAN), connections between THUNDER clients and THUNDER systems are direct. Any THUNDER client can connect to any THUNDER system. Connecting from a THUNDER client or THUNDER system to a THUNDER system is simply a matter of entering the internal IP address or name of the server. If there is more than one DNS name space in the WAN, the IP address can be used.

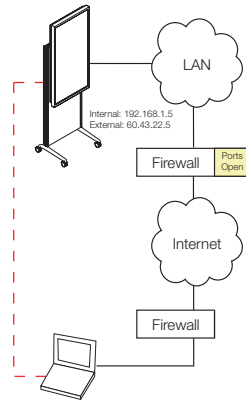
VPN connections are the same as being on the LAN or WAN. If a VPN connection is established from the outside (hotel room, airport, or another organization), any THUNDER device can talk to any other THUNDER device on the network.

THUNDER Clients on the Internet

In order for a THUNDER system to be accessible outside the organizations firewall, two things need to be done to the firewall:

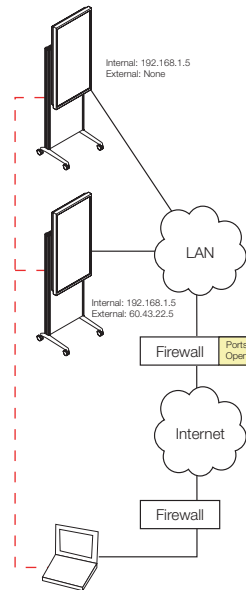
- An external static IP address must be assigned to the server. (In the example on the left, the internal IP address is 192.168.1.5 and the external address is 60.43.22.5.
- Three ports must be opened on the firewall to allow bi-directional communication to the server from outside the firewall.

If these changes are made (referred to “Ports Open” in these diagrams), a THUNDER client on the Internet may access the THUNDER system directly with the fixed IP address.



THUNDER Clients to Multiple Systems Behind a Firewall:

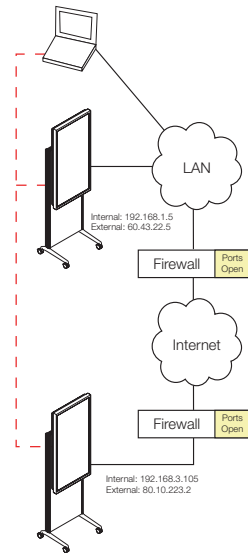
Once the firewall is properly enabled, multiple THUNDER systems in an organization can be added to the conference simultaneously, even if they do not have an external IP address.



THUNDER Systems through a Firewall:

Two or more THUNDER systems can communicate through firewalls. Each system must have an external IP address. In order for a THUNDER system to be accessible outside the organization's firewall, two things need to be done to the firewall:

- An external static IP address must be assigned to the system. (In the example on the right, the internal IP address is 192.168.1.5 and the external address is 60.43.22.5.)
- Three ports must be opened on the firewall to allow bi-directional communication to the system from outside the firewall.

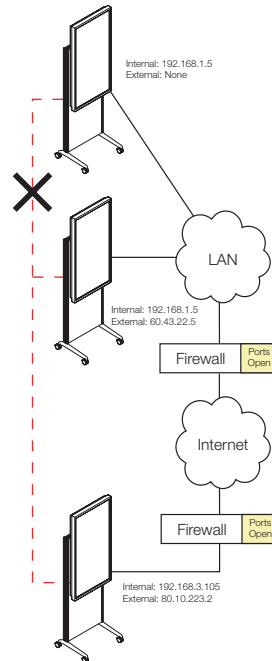


Multiple THUNDER Systems through a Firewall: (Incorrect)

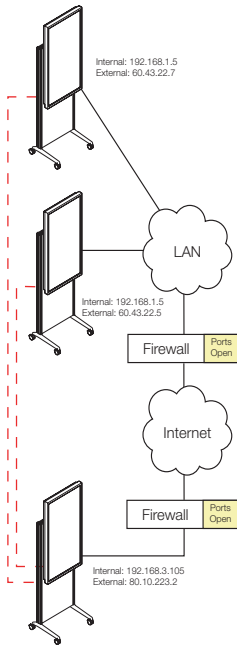
As mentioned above, each system must have an external IP address when multiple THUNDER servers are connected through a firewall.

Therefore, the example on the right will not work. The upper system does not have an external IP address. Although the connection may appear to have succeeded, the conference will perform erratically because one of the systems cannot communicate with another.

The example on the next page illustrates the correct way to configure this scenario.



Multiple THUNDER Systems through a Firewall: (Correct)



Each system must have an external IP address when multiple THUNDER systems are connected through a firewall. In addition, each THUNDER system must be able to reach all THUNDER systems in a conference by IP address. Therefore, external IP addresses should be used for all system connections when one system is located outside the firewall.

In the example on the right, each THUNDER system has an external IP address and has ports open to the Internet. The two systems in the top organization use the IP address of the lower organization's server (80.10.223.2) to establish the connection. When a conference is established this way, all data is available to every system and the conference works correctly.

THUNDER PRO OPERATING SYSTEM SECURITY

Unlike many network appliances available today, THUNDER Pro provides two levels of access, one for users and one for system management. On the easel connected to the THUNDER server, your users only see the THUNDER graphical user interface. They should never realize that the THUNDER system runs Windows XP beneath the application layer, nor should they care. However system administrators care very much.

Windows XP, like any modern operating system, evolves over time to provide security updates. Every organization has different corporate policies for maintaining virus protection, operating system updates, and so forth. By providing full access to the operating system, PolyVision encourages system administrators to customize the system to their own corporate IT policies.

THUNDER Pro comes factory-configured with the Windows Firewall turned on. This firewall should remain on unless other security measures are taken.

VIRUS UPDATES

In any networked environment, viruses are a threat. System administrators should make sure that they install the corporate virus protection before placing THUNDER on the network. It is important to tune the virus protection so it does not adversely affect the system performance.

SCREEN SAVERS

Screen savers are disabled on THUNDER Pro and should remain so on THUNDER Express systems as well. THUNDER can be configured to hibernate when left idle (refer to “Configuring Easel Options” on page 48). When hibernating, THUNDER Pro shuts down the projector and plasma display until the screen is touched again.

THUNDER PRO OPERATING SYSTEM AND SECURITY UPDATES

Operating system update policies vary by organization. By default, THUNDER Pro is configured to receive and install Windows XP updates automatically. If your IT policy prefers manual installation, or you use a third-party patch manager, you can easily reconfigure THUNDER to allow such configurations.

USER AUTHENTICATION

THUNDER should be placed on your domain and configured for your standard network authentication, if any. PolyVision does not recommend user-level authentication be enabled on THUNDER as it is designed as a walk-up-and-use device. There are no provisions for users logging into THUNDER. Therefore, the system should be set up with access to a nearby printer and other THUNDER systems but limiting access to other shared resources. If a user-level account is enabled, the THUNDER server should boot directly into the account so that no password is needed when the server reboots due to power failures or is otherwise restarted.

REMOTE ACCESS

Remote access of the THUNDER system through Remote Desktop Protocol (RDP) or virtual network computing (VNC) can aid remote maintenance of the system (e.g. installation of updates, backups, etc.). However, the usual security practices should be followed to prevent unauthorized access, such as strong passwords and named account access. (Remember that accessing the system remotely could lock out users, so be sure that the system is not in use.)

WEB PAGE ADMINISTRATION

There are two separate sets of administration web pages with each THUNDER system. One is provided by THUNDER and the other is located on the RoomWizard.

THUNDER provides a web interface with local and remote administration of system settings. These pages include options for setting the projector resolution and brightness level, configuring THUNDER to be a desktop application (THUNDER Express), usage tracking, and other system settings. These pages are only accessible through the use of an administrator password. For maximum protection, choose a password that cannot be easily guessed and would not be located in a dictionary.

RoomWizard also serves up web pages. Portions of these pages may be accessible by end users, depending on the installation. RoomWizard is deployed in either classic mode, which allows users to make reservations through RoomWizard web pages, or synchronized mode, where Microsoft Exchange, Lotus Notes or some other scheduling software is used to make reservations rather than RoomWizard's own user accessible web pages. In both modes, system administrators configure the RoomWizard through a password-protected web interface. Again, you should choose a password that cannot be easily guessed and would not be in a dictionary.

APPLICATION-LEVEL SECURITY

In addition to a secure network and operating system, THUNDER provides security at the application level to prevent unauthorized users from joining conferences and viewing or modifying sessions on the THUNDER server.

Depending on the environment you place THUNDER into, you may decide to enable none, some, or all of these security measures. Often the use of these measures changes from one use to the next. For instance, during a company-wide meeting, a user may want to enable access to any

participant. On the other hand, during a meeting to discuss new hires, the human resources department may choose to make the meeting completely private. A teacher or trainer may want to make the conference read-only to keep control over the content.

You may wish to set your own policy for the use the application-level security. Or, you may find that once the network and operating system security measures are in place, users naturally choose the appropriate security for their conference.

Each of the application-level security settings are described below.

CONFERENCE PASSWORD

When remote participants and other easels connect to an easel, a conference is formed. If a conference password is set, remote participants and easels are required to enter the password before joining in. The password can be changed from one conference to the next, can be left set to a single password, or can be removed entirely at the discretion of the host.

These security alternatives guarantee the maximum flexibility for the host. For sensitive information, a complex password can be used, while the password can be removed for open conferences.

READ-ONLY CONFERENCES

In some situations hosts want to allow participants to view a conference but not be able to alter or control the conference. This is often the case in classroom settings when many remote student participants or other classrooms are involved. To prevent remote control, a host chooses "Read Only" from the Conference menu.

In addition, this protection can be turned off or on at any time during a conference. For instance, a professor can make a presentation in a read-only conference and then remove the protection to take questions from the remote participants. Remote participants can then show a different page or add a comment to a professor's slide.

PRIVATE CONFERENCES

Private conferences are the strongest application-level security a host can apply. By making a conference private, no remote participants or other easels can join the conference. The conference is only viewable in the hosts room.

Some types of meetings are meant to be private, such as a board of directors meeting. By choosing “Private” from the Conference menu, the meeting host ensures that nobody can access the conference from outside the room.

Alternatively, users can make a conference private after some participants have joined. Participants who are connected to the conference remain connected, but new participants cannot join.

SESSION PASSWORDS

A session is set of saved pages on one or more THUNDER servers. (Think of them as documents on a traditional computer.) When sessions are saved, the host can specify a password to keep prying eyes out. By default, saved sessions take on the current conference password, but the host can specify a different password when saving the session for extra security. If there is no conference password, a session password can still be applied. This is useful in a conference which may have started with public information, but sensitive information was introduced during the meeting.

PORT BLOCKING CONSIDERATIONS

THUNDER makes use of a Flash Communications Server (FCS) for its low level communication between locations. FCS uses a specific set of ports in order to allow access through firewalls as needed.

FIREWALLS AND ATTACKS

Firewalls are essential for protecting networks from attacks. The rules for a firewall usually begin by denying all network traffic into and out of a network. Then additional rules open access under a few carefully selected circumstances. The rules you use depending on how you deploy THUNDER (refer to “Network Security” on page 13). The rules involve a number of settings:

- **Will the THUNDER server inside the firewall be reachable from the outside?** Can a computer connect to the THUNDER server on the local network; will the firewall pass the request to the THUNDER server or block it?
- **If a user can reach the THUNDER server inside the firewall using either UDP or TCP from the outside, what port or ports are accessible?** Port numbers are the addresses of applications running on the machine. For example, connecting to port 80 normally means the request goes to a web server, if one is available. A request to port 443 typically goes to a system that provides an SSL service that encrypts data as it passes it back and forth between the server and a remote client. Even though you may not specify a port number when using an application, all IP connections involve a connection request to a specific port number, using a specific basic protocol, such as UDP or TCP.

THUNDER uses the following ports:

- 80: THUNDER system administrator web pages and scanned documents
- 1935: Flash Communication Server traffic
- 8888: sharing remote desktops in a conference
- 11111: remote easel/client network status (checks that the connection is alive every few seconds)

NOTE:

All four three ports must remain open for THUNDER to operate properly.

- **Is a connection request initiated from outside the firewall or from inside your organization's network?** Most firewalls can distinguish between internal and external requests. These “stateful” firewalls keep track of network sessions and can permit network sessions (the flow of traffic back and forth across the firewall) that are only initiated from systems inside the firewall. Access to THUNDER servers from outside a firewall requires that THUNDER clients be able to initiate requests.
- **Does your firewall work at the application layer or at the network layer?** Most firewalls operate at the network layer and are unaware of the actual data or payload carried within network packets. Some firewalls work at the application layer and can examine the data carried within network packets and understand protocols such as HTTP and SMTP. You can configure application-layer firewalls to only

permit valid HTTP, ICMP, and SMTP traffic and exclude everything else.

Now consider each of these questions as you deploy THUNDER and determine how remote users connect to THUNDER:

- Which THUNDER servers (by IP address) should you allow remote users to connect to when the remote user (outside your firewall) initiates the connection?
- When a remote user is allowed to initiate a connection to the THUNDER server, which ports on the THUNDER system do you allow it to connect to, just the four mentioned above, or others?
- Are THUNDER systems within your firewall allowed to make requests to systems outside the firewall, such as to establish a connection to a remotely located THUNDER server?
- If THUNDER systems can request connections to outside the firewall, are they restricted to certain remote IP addresses?
- Should you use an application-layer firewall to examine data from outside the firewall to ensure it conforms to a protocol or format, like HTTP, SMTP or HTML?

Your decision for the type of network security used to deploy THUNDER determines the answers to these questions. Refer to “Network Security” on page 13.

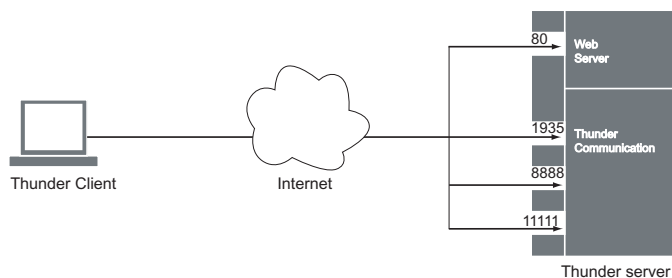
THUNDER's Flash Communication Server uses Real-time Messaging Protocol (RTMP) protocol to send and receive audio, video, and data in real time.

CONTROLLING CONNECTIONS INITIATED FROM OUTSIDE A FIREWALL

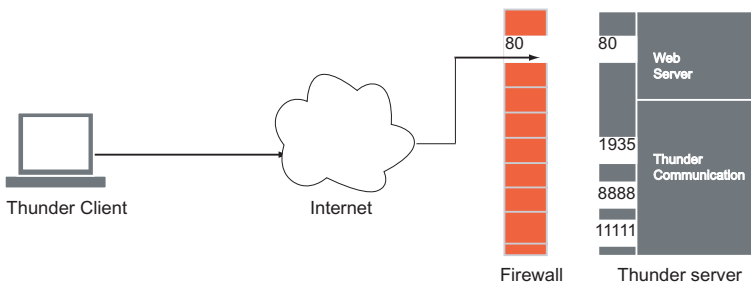
Normally, you configure a firewall to block connections initiated from outside except for connections to certain servers that must be available to the outside world. For example, you would allow access to port 80 on a web server (at a specific IP). Also, you would allow or open port 443 for SSL-encrypted web access.

These restrictions only affect THUNDER connections if you want to run the server inside a firewall and make it available to the outside world. By default, the server accepts connections from an outside THUNDER client or other servers on port 1935. That means port 1935 for the THUNDER server IP address must be open on the firewall. In addition, THUNDER uses ports 80, 8888, and 11111. These ports should also be opened on the firewall.

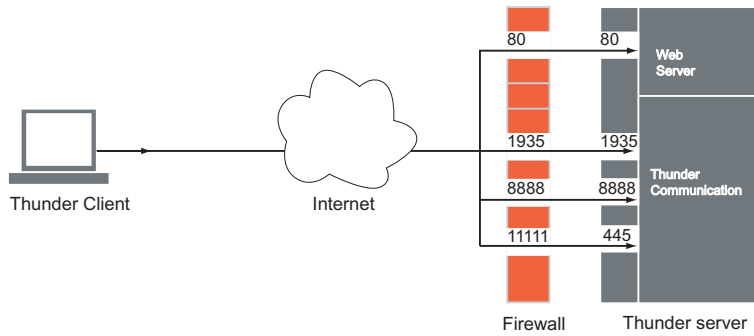
The example below shows a successful connection in a configuration where there is no firewall between a remote workstation and THUNDER.



The example below shows a deliberately oversimplified configuration in which a firewall permits access to port 80, but not to the requested port.



The example below shows the simplest solution, which is to open access through the firewall to port 1935, 8888, and 11111.

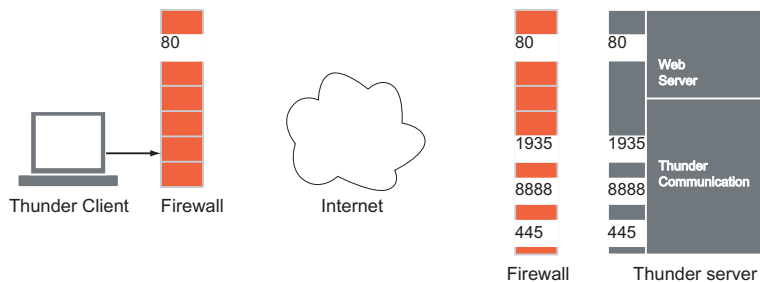


CONTROLLING CONNECTIONS INITIATED FROM INSIDE A FIREWALL

If a firewall lets THUNDER clients connect to any port on any system outside the firewall, there will be no connection problems.

Many organizations restrict the ports that local THUNDER clients can use to request connections outside the firewall. Some may restrict access only to the ports commonly used by web servers. The most common web server ports are 80 for HTTP and 443 for HTTPS. Web servers often use port 8080 as a secondary address for HTTP.

In the example below, a firewall that does not permit requests on port 1935 blocks client access to Macromedia Flash Communication Servers outside the firewall.



Open the three outbound ports to allow THUNDER client access to an outside server.

INSTALLING THUNDER EXPRESS SOFTWARE

SYSTEM REQUIREMENTS

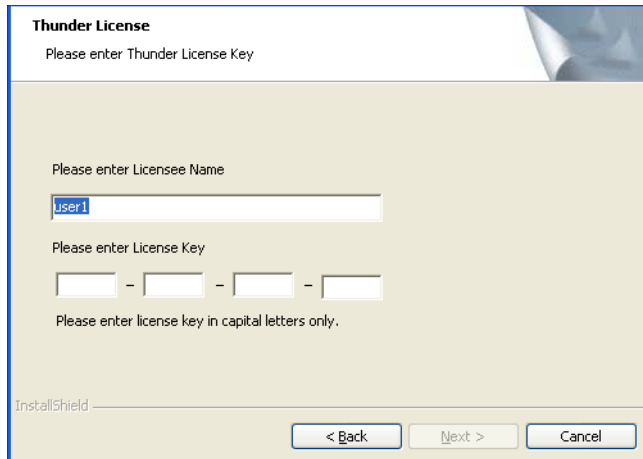
THUNDER Express is a software-only solution that provides the power of the THUNDER system with the flexibility to configure a variety of hardware components for input. THUNDER Express requires one of the following operating systems:

- Windows XP Professional
- Windows Vista Business, Ultimate, or Enterprise

INSTALLING AND RUNNING THUNDER EXPRESS

To install THUNDER Express on a computer:

- 1 Insert the installation CD ROM.
- 2 Run the set up program.
- 3 Click to accept terms of the license agreement and enter the THUNDER license key, which appears on the back of the jewel case containing the installation CD.



The image shows a 'Thunder License' dialog box with a blue border and a light beige background. At the top, it says 'Thunder License' and 'Please enter Thunder License Key'. Below this is a section for 'Please enter Licensee Name' with a text box containing 'user1'. Underneath is 'Please enter License Key' with four empty boxes separated by hyphens. A note at the bottom of this section says 'Please enter license key in capital letters only.'. At the bottom of the dialog, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'InstallShield' logo is visible in the bottom left corner.

- 4 Choose between installing “THUNDER Pro (Appliance)” or “THUNDER Express (Desktop)” for the type of installation. If you choose “THUNDER Pro (Appliance),” the system is configured as an appliance and you cannot run other applications alongside THUNDER, but the system is always ready for users to walk up and use. If you choose “THUNDER Express (Desktop),” the THUNDER system enables other applications to run alongside THUNDER, but users may need to start THUNDER software when they wish to use THUNDER.
- 5 Navigate through the Installation Wizard as instructed. Refer to “Configuring THUNDER for First Time Use” on page 37.

To run the THUNDER Express software:

- Double-click the THUNDER Easel icon on your computer desktop.

BOOTING THUNDER PRO FOR THE FIRST TIME

THUNDER Pro hardware installation is described in the *THUNDER Installation Guide*. The remaining THUNDER Pro installation steps require close coordination between the A/V installer and the local IT system manager. After all the THUNDER components are installed and the cables connected, the A/V installer and IT system manager work together to configure and test individual components until the system is up and running.

The remaining THUNDER Pro installation steps proceed in the following order:

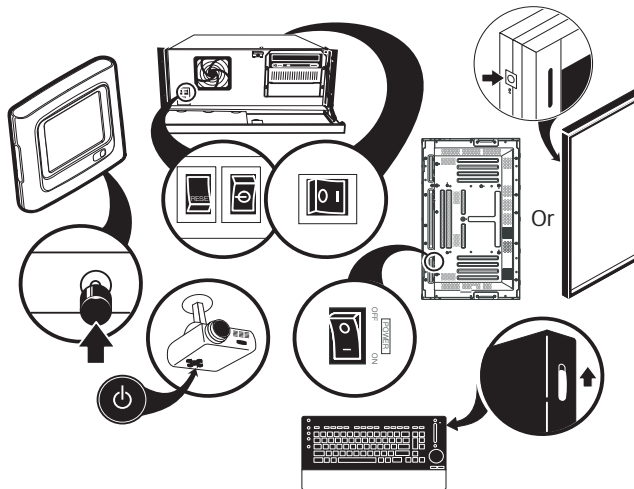
- 1 Locate the local IT system manager to work with that person through the remaining steps.
- 2 Together, power on the system components. Refer to “Booting THUNDER Pro for the First Time” on page 35.
- 3 Using the wireless keyboard, enter the Microsoft Windows key as prompted in a window that appears on the easel. Refer to “Entering the License Key” on page 37.
- 4 Enter the THUNDER license key when prompted. The number is located on a label on the THUNDER server. Refer to “Entering the License Key” on page 37.
- 5 Enter the Flash Communications key when prompted. The number is located on a label on the THUNDER server. Refer to “Entering the License Key” on page 37.
- 6 Enter the Desktop Sharing key when prompted. The number is located on a label on the THUNDER server. Refer to “Entering the License Key” on page 37.
- 7 Test and align the projectors. Refer to “THUNDER Pro: Configure the Projectors” on page 40.
- 8 Configure the plasma monitor. Refer to “THUNDER Pro: Configure the Plasma Monitor” on page 42.
- 9 Step through the configuration wizard that appears in the THUNDER easel. Refer to “THUNDER Configuration Wizards” on page 42.
- 10 Configure the video source input. Refer to “Configure the Video Input” on page 44.

When you boot THUNDER Pro for the first time, assure that all of the following power switches are turned on. (To reboot, refer to "Rebooting the THUNDER Pro System" on page 77.)

- **THUNDER server:** Flip the power supply switch near the power cord connection to the 1 position, then press the momentary power switch on the front of the chassis.
- **Plasma monitor:** Depending on which model you have: 1. Flip the power supply switch on the side or bottom of the plasma display. The power indicator flashes orange then flashes alternately green and orange. Do not touch the screen while the indicator is flashing, since automatic settings are being configured at this time. 2. Press the power button on the front of the plasma monitor frame.
- **RoomWizard:** Switch on the RoomWizard appliance power using the power button on the lower surface of the appliance.
- **Projectors:** Power on the projectors.
- **Keyboard:** Power on the wireless keyboard.

NOTE:

You should never need to turn on power manually again. THUNDER Pro is designed to remain constantly powered on and should not be turned off.



CONFIGURING THUNDER FOR FIRST TIME USE

The first time you start THUNDER, a series of Wizards guide you through the configuration process.

ENTERING THE LICENSE KEY

THUNDER PRO: ENTERING THE WINDOWS LICENSE KEY

NOTE:

For THUNDER Pro, use the easel and wireless keyboard to enter and change settings.

In THUNDER Pro, the server provides two levels of interaction. The easel software runs on top of a complete Windows XP system that you use for system controls.

The first time you boot up THUNDER, the screen displays a window requesting you to enter the Windows license key.

When you power on the THUNDER Pro for the first time:

- 1 Assure that the IT system manager is available.
- 2 Locate the Windows license key on a label on the front of the THUNDER server.
- 3 Type the license key into the window and continue. (THUNDER Pro provides a wireless keyboard for entering data. Refer to "About the THUNDER Pro Wireless Keyboard" on page 12.)

ENTERING THE THUNDER, FLASH, AND REMOTE DESKTOP SHARING LICENSE KEYS

NOTE:

THUNDER Pro: The license keys are located on a label on the front of the THUNDER server. Use the wireless keyboard to enter data. Make sure that the wireless keyboard is powered on. Refer to the THUNDER Pro Installation Guide for information about how to install the wireless keyboard.

THUNDER Express: The license keys are located on the back of the installation CD jewel case.

- 1 When requested, enter the THUNDER license key in the window that appears.

Thunder License

Please enter Thunder License Key

Please enter Licensee Name

user1

Please enter License Key

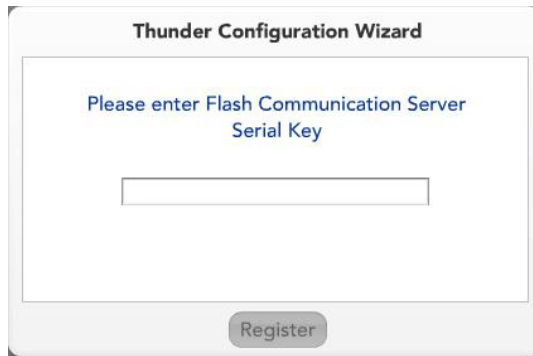
- - -

Please enter license key in capital letters only.

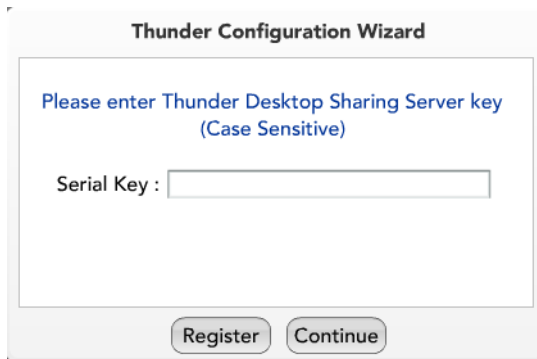
InstallShield

< Back Next > Cancel

- 2 Enter the Flash Communication Server Serial Key.



- 3 Enter the THUNDER Desktop Sharing Server Key. You must have a live Internet connection to validate this key but the connection can be removed once it is entered.



SYSTEM CONFIGURATION

You need to configure THUNDER as you would any other device on your network.

To perform system management tasks:

- 1 Exit the THUNDER software by pressing Alt-F4 on the keyboard. The screen now displays the Windows desktop instead of the THUNDER toolbar and workspace, and you can configure options as you normally would.

- 2 Choose **Start > Settings > Control Panel** and configure your network connection. Use a fixed IP address, if possible. Assure that the system is always on and that network login (if needed) is automatic.
- 3 If necessary, install or configure your antiviral and other security tools. Refer to “Planning Your Network Configuration” on page 13.
- 4 Map any drives required, for backing up THUNDER data, for example.
- 5 Enable remote desktop sharing or VNC, if appropriate. This step is only needed if you intend to manage the server remotely.
- 6 Rename the computer to a memorable name that relates to the location or identity of the THUNDER system (for example, EdisonRoom, or SecondFloorTHUNDER). No spaces are allowed in the computer name.
- 7 Configure your THUNDER options using the THUNDER administrator setup pages by opening Internet Explorer or other browser and entering “localhost” in the address line. These administrator setup options are described in full in the next section.
- 8 When you have completed network configuration, relaunch the THUNDER software by double-clicking the THUNDER Easel icon in the desktop.

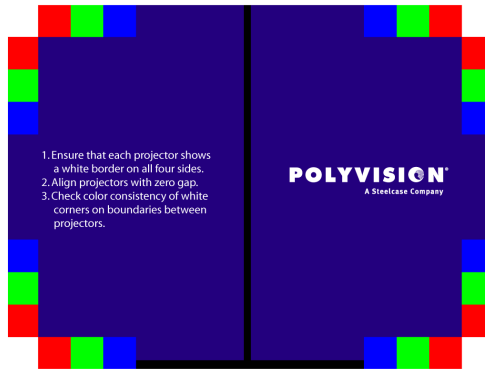
THUNDER Pro: CONFIGURE THE PROJECTORS

Before continuing with THUNDER Pro system configuration, make sure that all the THUNDER-enabled projections have the same appearance and are aligned across the wall. Projector adjustment procedures vary depending on the make and model of projectors in the THUNDER system.

To configure the THUNDER Pro projectors:

- 1 Press Alt-F4 to exit the THUNDER software. (For THUNDER Pro use the wireless keyboard provided with the system.) You see the Windows desktop. The THUNDER Pro desktop includes a projector

alignment pattern that provides color squares for color balance and a narrow white border around the image.



- 2 Make sure that the entire white border is visible on all four sides for all projectors.
- 3 Make sure that all the white borders are aligned across the tops and bottoms.
- 4 Make sure that the edges of the white borders touch so the projected images are immediately adjacent to each other.
- 5 Perform other adjustments for contrast and equalizing, depending on your projectors to ensure that they are the same size, color, etc.

THUNDER EXPRESS: CONFIGURE THE PROJECTORS

Before continuing with THUNDER Express system configuration, make sure that all the THUNDER-enabled projections have the same appearance and are aligned across the wall. Projector adjustment procedures vary depending on the make and model of projectors in the THUNDER system.

To configure the THUNDER Express projectors:

- 1 Make sure that the entire projection area is visible on all four sides for all projectors.
- 2 Make sure that all the projections are aligned across the tops and bottoms.
- 3 Make sure that the edges of the projections touch so the projected images are immediately adjacent to each other.

- 4 Perform other adjustments for contrast and equalizing, depending on your projectors to ensure that they are the same size, color, etc.

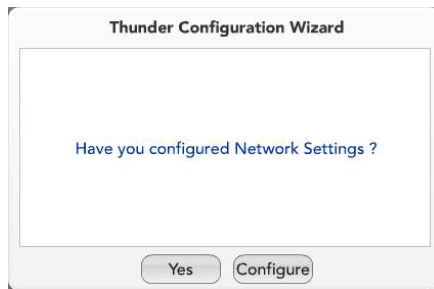
THUNDER PRO: CONFIGURE THE PLASMA MONITOR

Ensure that the image fills the THUNDER Pro plasma screen. By default, it should do so, but if you need to adjust it, use the remote control that comes packaged with the plasma monitor.

THUNDER CONFIGURATION WIZARDS

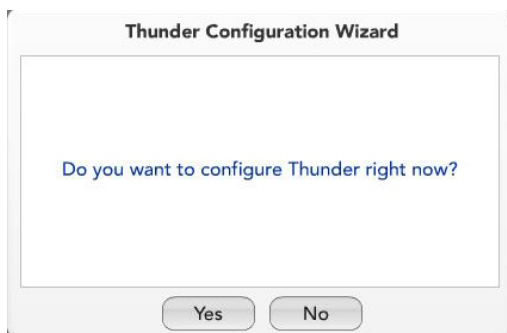
To continue to configure THUNDER:

- 1 Restart the THUNDER software by double-clicking the “THUNDER Easel” icon on the desktop. The THUNDER configuration wizards begin with connecting THUNDER to your network, if appropriate.



- 2 Click “Configure” to proceed through the network configuration wizard, or tap “Yes” if you are not using THUNDER over the network or you have already configured it.

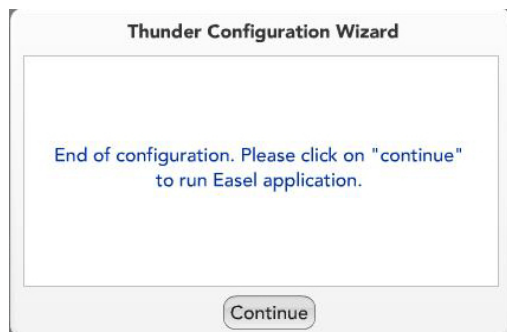
- 3 Click “Yes” to configure THUNDER setup options or “No” to postpone THUNDER setup. We recommend that you configure them now.



NOTE:

If you choose “Yes,” refer to “Configuring THUNDER Administrator Setup Pages” on page 45.

- 4 After configuring THUNDER, the final wizard launches the THUNDER application.



CONFIGURE THE VIDEO INPUT

THUNDER Express: Configure your video input now.

THUNDER Pro: If you installed optional DVD, VCR, or other video sources, video input configuration is required.

To do so:

- 1 To quit the THUNDER software, press Alt-F4.
- 2 Navigate to **Start > Programs > Osprey > Control Panel**.
- 3 Configure the Video Input to match your hardware installation. If you used the yellow RCA plug, choose "Composite."
- 4 Click "OK."
- 5 To launch the THUNDER software again, double-click the "THUNDER Easel" icon on the desktop.

CONFIGURING THUNDER ADMINISTRATOR SETUP PAGES

ENTERING AND EXITING THE ADMINISTRATOR SETUP PAGES

Configuring THUNDER is easy using web-based administrative setup pages. The first time you start THUNDER, you should configure at minimum the Projector and Easel setup page

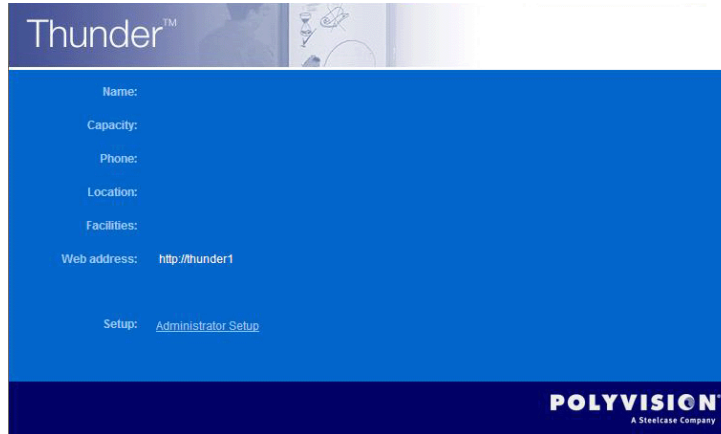
NOTE:

You can configure THUNDER from a computer that is connected to the same network and subnet as the THUNDER server. Before you can access the administrator setup pages, allocate an IP address to the THUNDER system.

To enter and exit the administrator setup pages:

- 1 Exit the THUNDER software by pressing Alt-F4 on the keyboard. The screen now displays a Windows desktop instead of the THUNDER toolbar and workspace, and you can configure options as you normally would.
- 2 Launch Internet Explorer or other browser. (The THUNDER Pro wireless keyboard includes cursor control and mouse buttons.)
- 3 Type "http://localhost" in the browser address line and press "Enter."

The THUNDER home page appears. (The fields are blank until you enter the information using the **Room** setup page.)



Thunder™

Name:

Capacity:

Phone:

Location:

Facilities:

Web address: <http://thunder1>

Setup: [Administrator Setup](#)

POLYVISION
A Steelcase Company

- 4 Click the “Administrator Setup” link at the bottom of the THUNDER home page. You are asked to enter a password.
- 5 Enter the administrator password. The default password is “**admin.**” You can change the password at any time using the **Security** setup page.
- 6 When you have completed network configuration, relaunch the THUNDER software by double-clicking the “THUNDER Easel” icon in the desktop.

CONFIGURING THE APPEARANCE OF THE HOME PAGE

When you enter the administrator setup pages, you see the **Room** setup page and tabs for the other setup pages. The **Room** setup page enables you to enter descriptive information about a THUNDER system and the room it occupies. This information appears in the THUNDER home page.

The screenshot shows the 'Room' setup page in the THUNDER administrator interface. The page has a blue header with the 'Thunder' logo and a navigation bar with tabs: Room, Easel, Projectors, Hardware, Security, and Status. The main content area is blue and contains form fields for Name, Capacity, Location, Phone, Facilities, and Photo. A 'Save' button is at the bottom left, and a 'Browse...' button is next to the Photo field. The footer is dark blue with the 'POLYVISION' logo and 'A Steelcase Company' text.

Name: The name used to identify the room.

Capacity: The number of people the room can hold.

Phone: The phone number of any phone in the room, such as a conference phone.

Location: Directions for finding the room.

Facilities: A list of room amenities, including the THUNDER and RoomWizard systems.

Photo: To customize the THUNDER home page you can add a photo or other graphic image. Enter the path to a GIF, PNG, or JPG graphic file or click "Browse" to navigate to the file.

Click the "Save" button when the **Room** setup page is complete.

CONFIGURING EASEL OPTIONS

The **Easel** setup page enables you to configure these options:

Room **Easel** Projectors Hardware Security E-Mail Usage Status

Easel Name: Thunder
This name is descriptive only and cannot be used to connect to the easel.

ID: TH1

Inactivity Timeout: 0 minutes
Enter 0 to disable hibernation.

Default Orientation:
☒ Portrait
☐ Landscape

Prompt Firewall: ☐ Warn on startup if firewall not configured for access
Displays a message asking to change firewall settings.

Thunder Desktop Application: ☐ Allow Thunder to be a desktop application
Adds the ability to operate the Thunder user interface as a window.

☒ Rotate the Windows desktop when the Thunder workspace rotates
Requires a Windows rotation-enabled video card.

☐ Smooth strokes from the local input device
Can improve the readability of handwritten text with some input devices.

Thunder Desktop Share Settings: ☐ Allow sharing of my desktop screen
☐ Allow control of my desktop screen

Upgrade Licensee Name: The Name of Licensee

Upgrade License Key: [][][][]

Save on this device

Easel Name: Enter a descriptive name for the system. It is a good idea to use the same name as the server name that you entered in your DNS. This name is displayed when the system is connected to a remote participant during a conference.

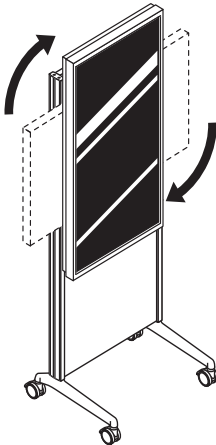
Three Letter ID: The easel toolbar includes an area where easels and other connected data sources are shown as icons that are individually identified by a three-letter monogram. Enter the three-letter ID for this server. It is a good idea to chose an ID that corresponds to the THUNDER Pro server name (i.e. the easel name) or the THUNDER Express computer name. For instance, if the server name is "LargeConferenceRoom," then the best ID might be "LCR."



three-letter IDs on the easel toolbar

Inactivity Timeout: THUNDER can be placed in hibernation after the period of inactivity that you specify here. When THUNDER hibernates, it turns off your plasma monitor and projectors, and can also control room lights, and other equipment if your room is so equipped. Set the value to zero to disable hibernation completely.

Default Orientation: The THUNDER Pro plasma monitor on the easel rotates between portrait and landscape orientation. Normally, THUNDER is used in portrait orientation similar to a flipchart but you can set the default orientation to landscape here.



Prompt Firewall: This option is checked by default to display a message that provides the option to temporarily change firewall settings to connect to a THUNDER session.

THUNDER Desktop Application: These options are checked by default for THUNDER Express installations. Check “Allow THUNDER to be a desktop application” to enable THUNDER to appear in an application window as well as in full-screen mode. Check “Rotate the Windows desktop when the THUNDER workspace rotates” to facilitate rotation from portrait to landscape mode. (THUNDER Express: Your video card must support the Windows control of desktop rotation. If Windows control of desktop rotation is not supported by your video card, this setting has no effect.). Check “Smooth strokes from the local device” to smooth handwriting with some THUNDER Express input devices.

THUNDER Desktop Share Settings: These settings enable or disable sharing the contents of the easel computer desktop with everyone in the meeting, similar to the way a remote participant using THUNDER client can choose to share their desktop. Checking the “Allow sharing of my desktop screen” box does not automatically show everyone the computer screen. You or someone in the conference must drag your source icon to the workspace to share your desktop in the conference. If someone does, you will know it because you see everything that happens in the workspace from the THUNDER client on your desktop. Checking the “Allow control of my desktop screen” box enables other conference participants to manipulate your shared desktop screen. For example, someone at the easel might scroll forward and backward through slides that are shared from your computer.

Upgrade Licensee Name: Enter the THUNDER licensee name. (A portion of the licensee name appears in the Status setup page.)

Upgrade License Number: If you choose to upgrade your THUNDER license to include more projectors, for example, use this space to enter the new license number which is provided for you at that time.

Click the “Save” button when the **Easel** setup page is complete.

CONFIGURING THE PROJECTORS

THUNDER supports connection of up to eight projectors, depending on your installed hardware and the THUNDER license that you purchased. Refer to “About the Projectors” on page 10. THUNDER supports connection of up to eight projectors. Use the **Projectors** setup page to configure projectors.

Model	IP Address	Projector Port	Resolution	Brightness / Color Adjustment (0-100%)			
				Red	Green	Blue	
External Control		RGB1	1024 * 768	100	100	100	Leftmost
None		RGB1	1024 * 768	100	100	100	
EPSON 830		RGB1	1024 * 768	100	100	100	
EPSON 835		RGB1	1024 * 768	100	100	100	
EPSON 1815		RGB1	1024 * 768	100	100	100	
EPSON 1715		RGB1	1024 * 768	100	100	100	
NEC NP1000		RGB1	1024 * 768	100	100	100	
NEC NP2000		RGB1	1024 * 768	100	100	100	
NEC LT380		RGB1	1024 * 768	100	100	100	
NEC WT610		RGB1	1024 * 768	100	100	100	
INFOCUS IN42		RGB1	1024 * 768	100	100	100	
SONY VPL-FE40		RGB1	1024 * 768	100	100	100	
SONY VPL-FX40		RGB1	1024 * 768	100	100	100	
HITACHI CP-X608		RGB1	1024 * 768	100	100	100	Rightmost
HITACHI CP-SZ608							

☐ Turn off projectors after inactivity

Delay: 0 seconds

Save on this device

POLYVISION
A Steelcase Company

Depending on the hardware you have installed, THUNDER recognizes projector positions from **Leftmost** to **Rightmost**. For each projector, you can independently set the **Model**, network **IP address**, **Resolution** and **Brightness**.

Choose a projector model from the drop down list for each installed projector. Options include a variety of projector models and:

- **None:** No projector is installed. THUNDER displays no image.
- **External Control:** The projector is under external control, such as by a Crestron room control system or manual remote control. THUNDER produces video output to this device.

Enter the network IP address for each projector. Where a separate room controller is used, the **IP Address** field should remain blank. Accidentally setting this field when a room controller is used results in unexpected behavior such as slow projector turn-on times.

Select the appropriate projector resolution from the drop-down list.

Select the red, green, and blue **Brightness** from the drop-down list to compensate for aging projector bulbs and to make the luminosity consistent across the projected images.

Turn off projectors after inactivity: Check this box if you want to shut off the projectors after a period of inactivity. You can set the inactivity timeout in the **Easel** tab.

Click the “Save” button when the **Projector** setup page is complete.

CONFIGURING PERIPHERAL HARDWARE

The THUNDER system can display information from scanned pages and video sources, can link with a room control system, and can print pages or the entire session (folder) of pages. Use the **Hardware** setup page to identify these peripherals.

Thunder™

Room Easel Projectors **Hardware** Security E-Mail Usage Status

Printer: hp officejet 5500 series

Plasma: Pioneer PDP504CMX

Video Source: Logitech QuickCam Pro 4000

Video Display: ☒ Show video input source with three-letter id: DVD

☐ Mute Audio when video input is paused

Video Resolution: 640 x 480

Frames Per Second: 6 Key Frame Interval: 15

Bandwidth (bytes per second): 120000 Quality of Video: 80

Scanner Display: ☒ Show scanner input source with three-letter id: SCN

Scanner Resolution (dpi): 100

Room Controller URL:

Save

Save on this device

Copyright (c) 2007, PolyVision Corporation

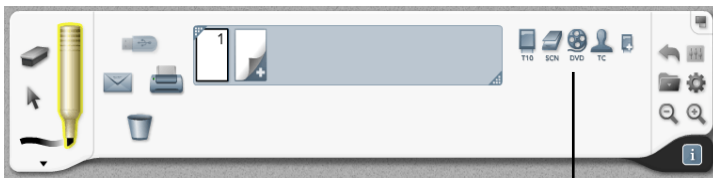
POLYVISION
A Steelcase Company

Printer: Identify the printer for THUNDER system users. This printer must be installed in the THUNDER server Windows control panel prior to configuring it here.

Plasma: Identify the plasma model for this THUNDER system. This setting has not effect if your system uses something other than a plasma display for the easel.

Video Source: Identify the video source for THUNDER. THUNDER supports only one video source at a time. The drop-down list shows all the available Windows video sources on your system so third-party video input hardware should be configured prior to changing this setting.

Video display: Show video input source with three-letter ID: The easel toolbar includes space where data sources are shown as icons that are individually identified by a three-letter ID. If one or more video sources are connected to the THUNDER room controller's inputs, check the box and give the toolbar icon a unique three-letter ID such as "DVD" or "VCR."



three-letter IDs on the easel toolbar

Video Resolution: Choose the appropriate resolution for your video source. This setting controls the quality of the picture sent to remote sites and therefore affects the bandwidth required. You can also enter specific **Frames per second**, **Key frame interval**, **Bandwidth**, and **Quality of video**.

Show scanner input source with three-letter ID: If you installed a scanner, check this box and add a three-letter ID (such as "SCN"). This monogram and a scanner icon appear in the easel toolbar. If a scanner is not connected, remove the check mark.

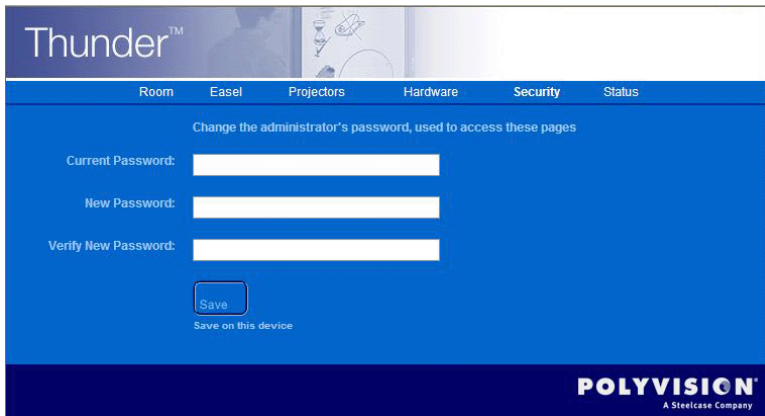
Scanner Resolution: Choose the resolution for locally scanned pages for transmission. High resolution images are transmitted more slowly. 200 dpi is the default setting.

Room Controller IP Address: If you are using a Crestron MP2E with THUNDER, enter the room controller IP address here. For example, “10.103.3.2/control/control.html.” This enables users to display and control room control features from the easel. Refer to “Diagnostics in the Room Control System” on page 71.

Click the “Save” button when the **Hardware** setup page is complete. You must restart the THUNDER easel application for changes to take effect.

CHANGING THE ADMINISTRATOR SETUP PASSWORD

A password is required to view and change administrator setup pages. The factory default password is “admin.” You should change the default password in the **Security** setup page.

The screenshot shows the THUNDER™ System Manager interface. At the top, there's a header with the THUNDER logo and a navigation bar with tabs: Room, Easel, Projectors, Hardware, Security, and Status. The Security tab is selected. Below the navigation bar, the page title is "Change the administrator's password, used to access these pages". There are three input fields: "Current Password:", "New Password:", and "Verify New Password:". Below these fields is a "Save" button. At the bottom right, the POLYVISION logo is displayed with the text "A Steelcase Company" underneath it.

To change the password:

- 1 Enter the current password. (The default password is “admin.”)
- 2 Enter the new password.
- 3 Enter the new password a second time to verify it.
- 4 Click the “Save” button.

CONFIGURING EMAIL

THUNDER can interact your SMTP and LDAP servers to enable users to email THUNDER pages. In addition, THUNDER usage tracking can automatically send email with periodic usage tracking information.

NOTE:

These settings only apply to the transmission of pages manually sent from THUNDER. To enable One-Click Publishing, where pages are sent automatically at the end of meetings, the RoomWizard must be configured for an email server as well. Refer to "Configuring RoomWizard to Integrate with THUNDER" on page 59.

Use the **Email** setup page to identify the SMTP server for sending THUNDER pages in email and for usage tracking email, and to identify the LDAP server for email address lookup.

Thunder™

Room Easee Projectors Hardware Security **E-Mail** Usage Status

SMTP Server:

SMTP Username:

SMTP Password:

LDAP Server:

LDAP Port:

LDAP Username:

LDAP Password:

LDAP Search base:

Save on this device

Copyright (c) 2007, PolyVision Corporation

POLYVISION
A Steelcase Company

SMTP Server: Enter the server address, username, and password of the SMTP server for sending THUNDER pages in email and THUNDER usage tracking emails. This address usually points to an internal SMTP server on your LAN.

LDAP Server: Enter the server address, port ID, username, password, and search base to provide users with the ability to validate and look up email addresses from the corporate address book with access to your network LDAP server.

Click the “Save” button when the **Email** setup page is complete. You must restart the THUNDER easel application for changes to take effect.

CONFIGURING USAGE TRACKING

THUNDER usage is tracked for accounting purposes. The **Usage** page provides the details of the accounting agreement that fixes charges from PolyVision based on usage. Usage tracking agreements can vary; check with your contract to determine the details for your installation.

Accounts Payable Email Address: Enter the email address for accounts payable communication or your own address. This address will receive periodic usage reports from this server.

Frequency of Emails: Choose from a drop down list of reporting frequencies.

Send a copy to PolyVision: Check this box to send a copy of each usage report to PolyVision.

Billing Rates: For the listed rates, enter the charges for each type of connection. Some values may be zero. Enter each rate in the same currency and select the currency used.

Computer Connections: Each time a remote (laptop) user is connected to this easel, it counts as one laptop connection. When the connection is established, the count is immediately increased incrementally. Any successful reconnection a user makes counts as another connection.

Easel Connections: Each time another easel is connected to this easel, it counts as one easel connection, regardless of how the connection is made (from this easel outbound, or inbound to this easel). When the connection is established, the count is immediately incremented.

Computer Connection Duration: The length of time (duration) of the connection from each remote (laptop) user to the easel is logged. If there are 20 laptop users connected in a session for one hour, 20 hours of usage are logged. Connect duration is logged whether or not there is any activity over the connection (someone goes home at night with the laptop still connected).

Easel Connection Duration: The length of time (duration) of the connection from each other easel to this easel is logged. If there are 20 easels connected in a session for one hour, 20 hours of usage are logged. Connect duration is logged whether or not there is any activity over the connection (someone goes home leaving the easel still connected).

Active Easel Usage: The amount of time that the easel is actively in use is monitored and logged. Active use starts when there is any mouse, stylus, or finger activity on this easel. It ends when there is no activity for at least 10 minutes. (The 10 minute dead-time is *not* considered part of the active usage duration.)

For example, if two laptop users connect into an easel remotely when there is nobody present in the easel room, their usage of that easel is considered active use as long as they are manipulating the user interface in some way.

CHECKING THUNDER USAGE STATUS

The **Status** page provides information about THUNDER system administration and statistics related to THUNDER usage.

The screenshot shows the Thunder Status page with a blue background. At the top, there is a navigation bar with links: Room, Easel, Projectors, Hardware, Security, E-Mail, Usage, and Status. The main content area displays the following information:

- Version No: 2.3.8
- Licensee Name: A Thunder 10
- License Key: F3Z37
- No of enabled Projectors: 4
- Date/Time: Thursday, December 13, 2007 01:20:33 PM
- Up Since: Thursday, December 13, 2007 12:59:16 PM

	This Period	Total
Total computer connections made:	583	583
Total easel connections made:	96	96
Total computer connection duration:	158,313	158,313 minutes
Total easel connection duration:	30,405	30,405 minutes
Total active easel use duration:	5,774	5,774 minutes

At the bottom, there is a footer with the text: Copyright (c) 2007 PolyVision Corporation and the PolyVision logo, which is a Steelcase Company.

Version No: Displays the current software version.

Licensee Name: Displays the name of the system to which this license is applied.

License Key: Displays a portion of the THUNDER license key for this system.

No. of enabled Projectors: Displays the number of projectors licensed for this system.

Totals and accumulated usage statistics are provided on this page.

CONFIGURING ROOMWIZARD TO INTEGRATE WITH THUNDER

Refer to the *RoomWizard System Manager Guide* for information about installing and configuring RoomWizard.

RoomWizard is a web-based room scheduling appliance that integrates with THUNDER to provide the email options in THUNDER. (RoomWizard should be installed and ready to use when the A/V installer hands off the THUNDER system. If RoomWizard with One-Click Publishing is not properly installed, the email features provided in THUNDER are disabled.)

When a meeting organizer reserves a THUNDER room using RoomWizard, the people listed in the reservation form as invitees are the individuals who receive the emails sent during the meeting.

Each RoomWizard appliance is a “network node” with its own connection to the LAN. To configure the integration the RoomWizard that is installed outside the room with THUNDER:

- 1 Go to the RoomWizard appliance and press the “i” button on the front panel. Roomwizard displays its own unique IP address. (If the RoomWizard’s IP address is not yet configured, refer to the *RoomWizard System Manager Guide*.)
- 2 Using a computer on the same network as RoomWizard, browse to the RoomWizard’s IP address. You see the RoomWizard’s home page.
- 3 Click the **Administrator Setup** link at the bottom of the home page.
- 4 Enter the RoomWizard password. The default password is “roomwizard.”
- 5 Navigate to the **Room > Whiteboards** tab.
- 6 Add the IP address for the THUNDER server. Also enter IP addresses of any CopyCam or Impulse LTX whiteboard(s) associated with this meeting room.
- 7 Navigate to the **Device > Email** tab to specify the SMTP and LDAP servers used for email functions. Refer to the *RoomWizard System Manager Guide*.
- 8 Click “Save on THIS Wizard.”

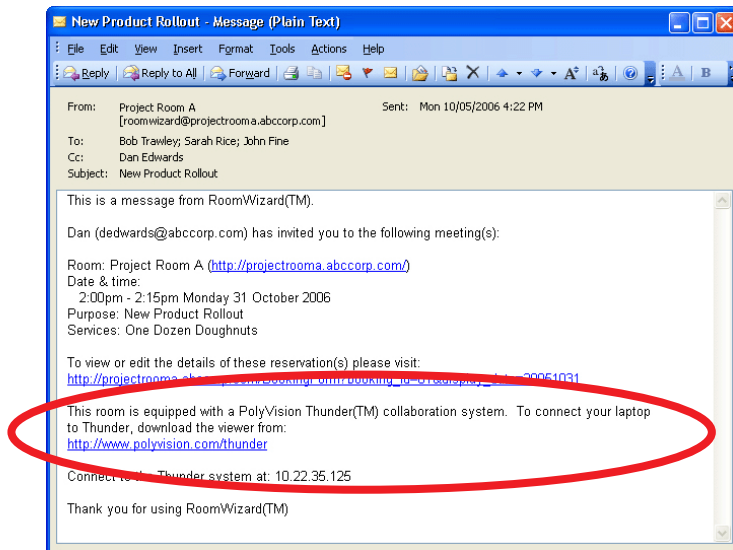
THE THUNDER CLIENT SOFTWARE

OBTAINING THE CLIENT SOFTWARE

Participants who want to join a THUNDER conference using their own computer require THUNDER client software installed on their computer.

THUNDER provides three ways for participants to receive the THUNDER client software:

- When a meeting organizer reserves a THUNDER room using RoomWizard, meeting invitees receive a reminder email that includes a link to download THUNDER client software from PolyVision.



- Participants can download the same THUNDER client software by visiting the PolyVision website at: www.polyvision.com/thunder.
- You can also post the THUNDER client software on an internal ftp server or other location where participants can download it. In addition, the THUNDER client can be included in your standard computer installation so that all employees or students have access to your THUNDER systems.

INSTALLING THE CLIENT SOFTWARE

To install the THUNDER client software on a computer:

- 1 Download the software to your computer.
- 2 Double-click the downloaded file to start installation.

PLACING THE THUNDER CLIENT SOFTWARE ON YOUR OWN SERVER

You can obtain the THUNDER client software from the PolyVision web site at: www.polyvision.com/thunder.

GETTING SOFTWARE UPDATES

THUNDER system managers regularly receive notification of software updates. Updates are available at www.polyvision.com.

UPDATING THE THUNDER SOFTWARE

To update the THUNDER software:

- 1 Exit the THUNDER software by pressing Alt-F4 (For THUNDER Pro, use the wireless keyboard).
- 2 Uninstall the current THUNDER software using the Windows “Add/Delete Programs” Control Panel.
- 3 Download and unzip the software update file.
- 4 Execute “setup.exe.” A new THUNDER icon appears in the desktop.
- 5 Double-tap the THUNDER icon in the desktop to open the software.

UPDATING THUNDER CLIENT SOFTWARE

To update THUNDER client software for a remote participant’s computer:

- 1 Remove the current THUNDER client software by uninstalling the “THUNDER” application using the Windows “Add/Delete Programs” Control Panel.
- 2 Download the new version.
- 3 Double-click the downloaded file. A new THUNDER icon appears in the desktop.

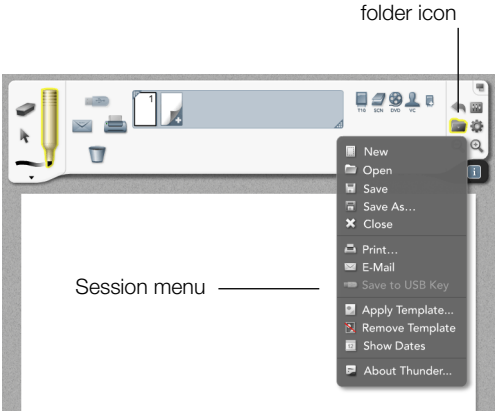
SYSTEM MAINTENANCE

REMOVING OLD SESSIONS

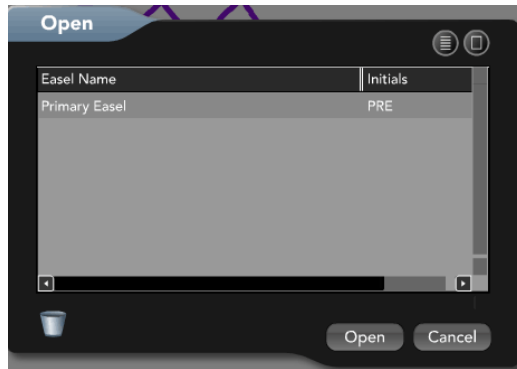
A regime of regular system maintenance is recommended for your THUNDER server. THUNDER sessions accumulate continually and are not deleted when software updates occur.

To remove old sessions:

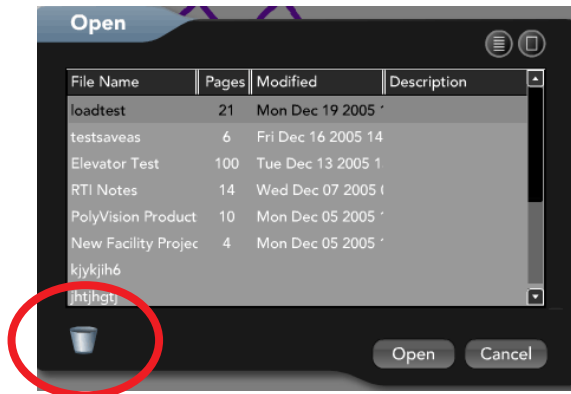
- 1 Tap the folder icon on the easel toolbar to open the “Session” menu.



- 2 Tap "Open." If the easel is conferencing with other easels, you see a list of the conferenced easels. If the easel is not in a conference, only your easel is shown.



- 3 Tap the name of the easel you want to delete sessions from and choose "Open". You see a list of all the sessions saved on that easel.



- 4 Drag unneeded sessions to the trash can icon in the Open dialog.

MAKING SESSION BACKUPS

THUNDER sessions can include valuable information that should be backed up regularly.

To back up THUNDER sessions:

- 1 Exit the THUNDER easel software by pressing Alt-F4 using the wireless keyboard or access the hard drive remotely through the network.
- 2 Navigate to C:\Program Files\Macromedia\Flash Communication Server MX\application\THUNDER.
- 3 Make a copy of the "THUNDER" folder and back it up in a conventional manner to a secure location on your network.
- 4 Restart the THUNDER software by double-clicking the THUNDER icon in the desktop.

UPDATING WINDOWS

Be sure to update Windows software and maintain Internet Explorer software on a regular basis.

To update Windows:

- 1 Exit the easel software by pressing Alt-F4 using the wireless keyboard. You see a Windows desktop.
- 2 Manage the operating system as you normally would any Windows system. Check for Windows updates at www.microsoft.com.

PERFORMING VIRUS CHECKS

THUNDER does not include any anti-virus software. As part of the installation, you should install such software.

Be sure to scan the system, update anti-virus software, and update virus definitions on a regularly scheduled basis as you normally would any Windows system.

CARING FOR THE THUNDER PRO PLASMA MONITOR

Care for the THUNDER Pro plasma monitor using the following guidelines:

- Never use solvents such as benzene or thinner.
- Never use liquids near sensitive electronics.
- Remove dust and dirt by lightly wiping with a soft dry cloth.
- Do not rub with a facial tissue or other abrasive materials.
- If necessary, slightly moisten a soft cloth with neutral detergent diluted with water to clean the monitor. Make sure that the liquid does not seep into sensitive system electronics.
- In humid conditions, wipe off condensation with a soft, dry cloth.
- With a slightly moist cloth, gently wipe the diagonal surfaces of the touch screen. Immediately dry the surface. Make sure that the liquid does not seep into sensitive system electronics.

CARING FOR THE THUNDER PRO SERVER

Care for the THUNDER server as follows:

- Every month, remove dirt from the vent on the rear of the server using a vacuum cleaner with low suction.
- Assure that the THUNDER server is in a well-ventilated space.

CARING FOR PROJECTORS

Care for projectors using instructions provided with the projectors and also consider the following:

- Turn off projectors when not in use unless your system is configured to turn them off automatically when THUNDER is in hibernation mode.
- As bulbs on projectors age they can experience a shift in brightness. You can compensate for this in a variety of ways. Refer to “Maintaining Projector Color Balance” on page 67.
- Projectors may need realignment to assure that projected pages all line up precisely on the wall. To restore projector alignment, refer to “Re-aligning the Projectors” on page 67.

- THUNDER's projectors may be shared with other video sources and thus may display a warning in the easel toolbar. Refer to "Recovering Shared THUNDER Projectors" on page 67.

RE-ALIGNING THE PROJECTORS

If projector alignment needs to be restored, use the projector's remote control and user guide to adjust keystone and alignment until all the projected pages align across the tops and there are no gaps between projected pages.

MAINTAINING PROJECTOR COLOR BALANCE

Projector color shifts as bulbs age. To restore projector color balance:

- 1 Open a new THUNDER session and add blank white pages for all the projectors by tapping the white add page icon once for each new page.
- 2 Using the projector's remote control and user guide, adjust color balance until all the projected pages are bright white.

NOTE:

*Many projectors have built-in color and brightness adjustments. If these adjustments are not available, use the **Projectors** page of the administrator setup pages to adjust projector brightness so all projectors display consistently. Refer to "Configuring the Projectors" on page 51.*

RECOVERING SHARED THUNDER PROJECTORS

THUNDER projectors can be shared with other video sources that are not part of the THUNDER system, such as video conferencing systems, a camera, or a computer for PowerPoint presentations, making them unavailable to post THUNDER pages on the wall.

NOTE:

THUNDER can only detect shared projectors when Thunder is configured to control projects. Refer to "THUNDER Pro: Configure the Projectors" on page 40 or "THUNDER Express: Configure the Projectors" on page 41.

The THUNDER easel toolbar makes it easy to recover the use of shared THUNDER projectors. When a THUNDER projector is shared, the sliding projection box shrinks to indicate that fewer pages are being posted and an icon appears to alert you that the projector is unavailable for THUNDER. You can recover shared THUNDER projectors at any time.

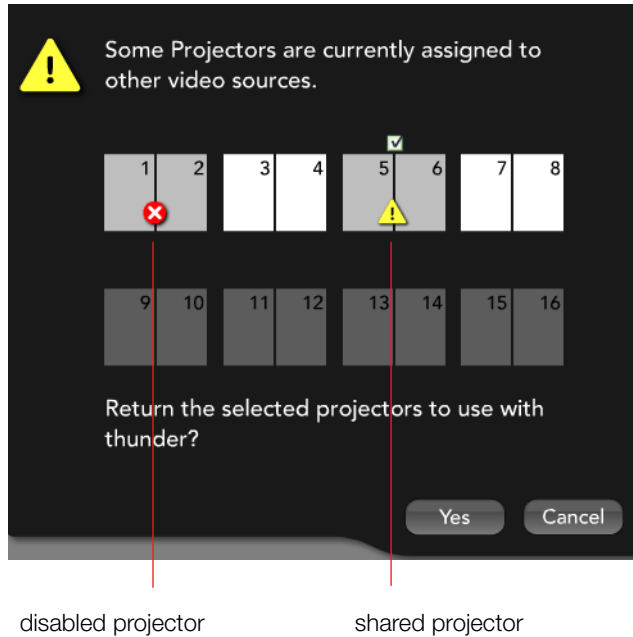


NOTE:

The number of pages you can "post" on the wall depends on the number of projectors in your license. The maximum is eight projectors and 16 projected pages, but there is no limit to the number of pages that you can create.

To recover a shared THUNDER projector:

- 1 Click the warning icon in the toolbar. You see a dialog box that identifies each projector's status. Shared THUNDER projectors are indicated by a warning symbol and check mark.



NOTE:

Disabled projectors are indicated by a red "X."

- 2 Click to remove the check mark for each shared projector you want to recover for use by THUNDER.
- 3 Click "Yes."

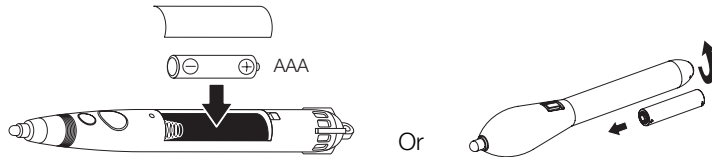
CARING FOR THE THUNDER PRO STYLUS

The THUNDER Pro stylus is battery operated and has a replaceable tip.

STYLUS BATTERY REPLACEMENT

To replace the battery:

- 1 Open the battery compartment.
- 2 Add one AAA battery.



STYLUS TIP REPLACEMENT

If the tip is worn replace it to avoid damaging your monitor. Damage due to a worn tip is not covered by your warranty.

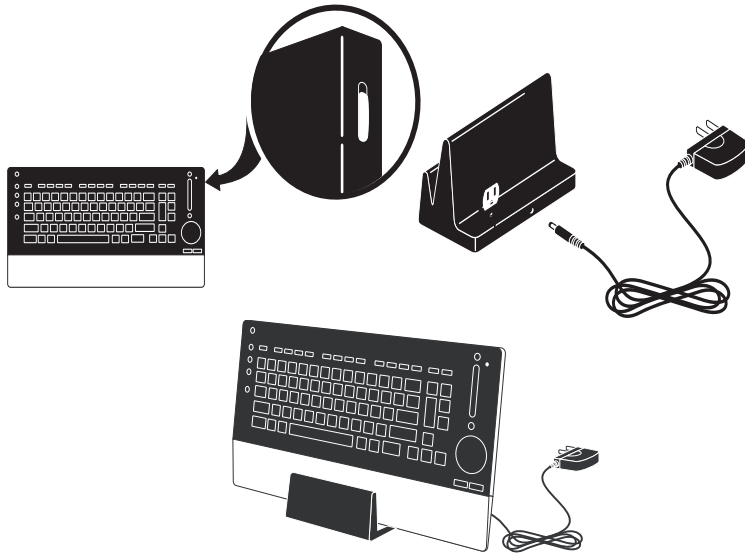
Two spare tips are included with THUNDER. To order additional tips, contact PolyVision at 1.800.620.POLY or +1.678.542.3100.

To replace the stylus tip:

- 1 Pull out the damaged or worn stylus tip.
- 2 Push in the replacement tip.

CARING FOR THE THUNDER PRO WIRELESS KEYBOARD

The wireless keyboard should be stored in its charging base. The keyboard should always be left “on” and the charging base plugged into a power outlet.



DIAGNOSTICS IN THE ROOM CONTROL SYSTEM

THUNDER integrates with a room control system, if one is installed, giving users control of options from an interface on the THUNDER toolbar. The system manager links THUNDER with the room control system using the **Hardware** tab of the administrator setup pages. Refer to “Configuring Peripheral Hardware” on page 52.

Refer to the *THUNDER User Guide* for details about using the THUNDER room control interface. The room control **Diagnostics** tab provides helpful information that enables you to troubleshoot potential problems or perform regular maintenance.

ROOM CONTROL DIAGNOSTICS

To view the room control diagnostics:

- 1 Tap the room control icon in the THUNDER easel toolbar.

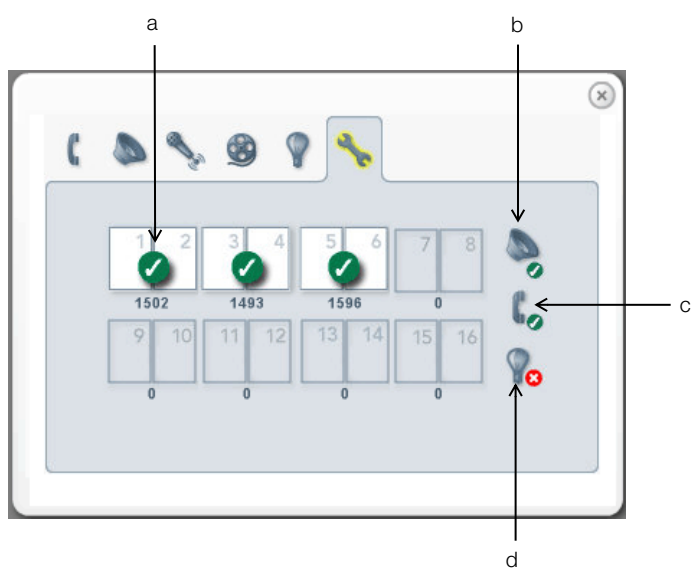


- 2 Tap the **Diagnostics** tab.

NOTE:

This window is blank if room control options are not installed.

The **Diagnostics** tab presents information concerning:



- a **Projector status:** For each projector, you see the number of hours the bulb has been in use. The lamp indicator turns to red when the bulb has reached 75% of its life. A check mark indicates normal communication with the THUNDER server and there are no problems detected. A red "X" indicates that the system is communicating but there is a problem with the projector. A warning symbol indicates no communication to the projector.
- b **Audio status:** A check mark indicates that there is normal communication with the THUNDER audio processor and there are no problems detected. A red "X" indicates that the audio processor is communicating but there is a problem. A warning symbol indicates no communication with the audio processor.
- c **Audio conferencing status:** A check mark indicates that there is normal communication with the THUNDER audio conferencing system and there are no problems detected. A red "X" indicates that the audio conferencing system is communicating but there is a problem. A warning symbol indicates no communication with the audio conferencing system.
- d **Lighting status:** A check mark indicates that there is normal communication with the lighting controller and there are no problems detected. A red "X" indicates that the lighting controller is communicating but there is a problem. A warning symbol indicates no communication with the lighting controller.

TROUBLESHOOTING

PROBLEM	SOLUTION
System is not printing when pages or thumbnails are dragged to the printer icon.	Make sure that the correct printer is chosen in the administrator Hardware setup page on the easel. Refer to “Configuring Peripheral Hardware” on page 52.
Writing on printed pages is too large.	Try setting the print options on your printer to “4-up,” to place four handwritten pages on a single printed page.
The easel’s touch screen coordinates are “off” by about a quarter of an inch.	The easel’s plasma display needs to be auto adjusted. Press the “Auto Setup” button on the right edge of the plasma display. (If the plasma display is in portrait orientation, these controls will be on the bottom of the bezel.) This will properly center the plasma display image within the plasma monitor.
Unable to establish a conference connection from a laptop to the easel.	Make sure that there is a valid network connection between the laptop and easel. Try a network ping. If the ping is successful, make sure that ports 1935, 8888, and 11111 are open in the firewall on both the THUNDER server and any intervening firewalls.
Unable to hear any audio, such as flipping pages, DVDs, or Help.	<ul style="list-style-type: none">• Make sure that the room’s audio amplifier is turned on.• Adjust the device’s volume by tapping the room control icon, tapping the audio tab, and then sliding the indicator up for the device.• Make sure that the mute icon in the room control audio tab is not selected for that device.• Check that the audio from the rear of the THUNDER server is properly connected to your audio amplifier. (Refer to the <i>THUNDER Hardware Installation Guide</i>, if necessary.)

PROBLEM	SOLUTION
Audio is produced by the flipping of pages but not by the DVD player (or another video input source).	<ul style="list-style-type: none"> • Adjust the source volume by tapping the room control icon in the THUNDER easel toolbar, tapping the audio tab, and then sliding the indicator up for the device. • Make sure that the mute icon is not selected for the device in the room control audio tab. • Make sure that the audio cables are connected from your video source to the video input breakout cable in the back of the THUNDER server. (Refer to the <i>THUNDER Hardware Installation Guide</i>, if necessary.) • If cables are connected, quit the THUNDER easel software (press Alt-F4), navigate to Start > Programs > Osprey > Control Panel and make sure that the correct audio source is enabled for the video input.
When a DVD video source is dragged into the workspace, audio is heard but no video is seen.	<ul style="list-style-type: none"> • Make sure that the desired video source is selected in the room control video tab in the THUNDER easel toolbar. • Make sure that the video cables are connected from your source to the video input breakout cable in the back of the THUNDER server. (Refer to the <i>THUNDER Hardware Installation Guide</i>, if necessary.) • If cables are connected, quit the easel software (press Alt-F4), navigate to Start > Programs > Osprey > Control Panel and make sure that the correct video source is enabled for the video input.
The plasma monitor displays the correct image, but the touch-screen is not responding to the stylus or finger.	<ul style="list-style-type: none"> • Make sure that the touch-screen USB cable is connected at the upper left corner (from the back) of the plasma monitor. • Ensure that the all USB cables are connected to the hub inside the back of the easel (remove the easel back to access the hub). • Ensure that the CAT5 cable from the easel to the CAT5-to-USB converter at the back of the THUNDER server is properly connected. • If cables are properly connected, call your THUNDER installer or PolyVision technical support at 1.800.620.POLY.

PROBLEM	SOLUTION
No picture appears on the plasma monitor, and a yellow LED is visible in the corner of the plasma monitor.	<ul style="list-style-type: none"> • Touch the monitor to wake up the system. If there is still no activity, press the Standby/On button on the plasma monitor to turn on the display. • Check the serial cable between the server and the plasma monitor to be sure it is properly connected. (Refer to the <i>THUNDER Hardware Installation Guide</i>, if necessary.)
No picture appears on the plasma monitor, and there is no LED visible on the plasma display.	<ul style="list-style-type: none"> • Make sure that the power toggle switch on the bottom (left side) of the plasma is on. • Check that the power cable for the easel is plugged into the wall. • Make sure that the power connector inside the easel (remove the easel back) has not come loose and is secured with a cable tie. • Make sure that the power connector is fully seated in the back of the plasma monitor. • Make sure that the power outlet is switched on.
RoomWizard is not sending email at the end of the meeting.	<ul style="list-style-type: none"> • Make sure that a valid email address is specified for the invitees when making the room reservation in RoomWizard. • Ensure that the checkbox "Send Whiteboard Notes" on the meeting reservation is checked. • Make sure that the SMTP server is configured on the RoomWizard administrator setup pages. • Ensure that the RoomWizard points to the correct IP address for the THUNDER server under the Whiteboard tab in the RoomWizard administrator setup pages. • Ensure that the date and time match between the THUNDER system and the RoomWizard.
The plasma display turns off during hibernation, but the projectors do not.	Check with your local THUNDER integrator to ensure that projector power control is enabled.

REBOOTING THE THUNDER PRO SYSTEM

It is recommended that all components in the THUNDER Pro system should be connected through the rack to a UPS power switch so all restart together when you reboot.

To reboot THUNDER Pro:

- 1 Power off the entire THUNDER Pro system using the UPS in your rack.
- 2 Wait 10 seconds.
- 3 Switch on the UPS power again.

The THUNDER Pro easel displays the underlying Windows XP desktop for approximately 1 minute while it powers on. Be patient while the system starts up.

APPENDIX A: THUNDER EXPRESS HARDWARE CONSIDERATIONS

THUNDER EXPRESS OVERVIEW

THUNDER Express is a software-only solution for collaborating using THUNDER. THUNDER Express runs with any of the following operating systems:

- Windows XP Professional
- Windows Vista Business, Ultimate, or Enterprise

THUNDER Express can host a conference just as THUNDER Pro. THUNDER client users can connect to a THUNDER Express system or a THUNDER Pro system.

CONFIGURATION STRATEGIES

THUNDER Express software provides the power of global multimedia communication with highly customized hardware configurations. THUNDER Express opportunities can be divided into two general types:

- **Collaborative:** participants collectively develop or present information using the THUNDER Express virtual flipchart to share, view, and mark up information as a group.
- **Presentation:** participants view information that is provided to them by a lecturer or leader who uses the THUNDER Express virtual flipchart to organize information privately and then present it.

THUNDER Express provides flexibility to create a system that can maximize collaborative or personal experiences for small group environments. For example, THUNDER Express installations targeted at more collaborative opportunities might include a large interactive workspace such as a Walk-and-Talk Interactive Whiteboard, a touch-sensitive plasma monitor or other large format, highly visible, and highly interactive display.

Alternatively, when THUNDER Express is intended for presenting information rather than interacting with information, the installation might include the PolyVision IP 17 Interactive Panel or a tablet PC for the lecturer or presenter to access and display information from a variety of media.

As with THUNDER Pro, when team members, students, board members, or others need to participate remotely, they can connect to the THUNDER Express session using THUNDER client which they can download freely.

USING THUNDER EXPRESS WITH PROJECTORS

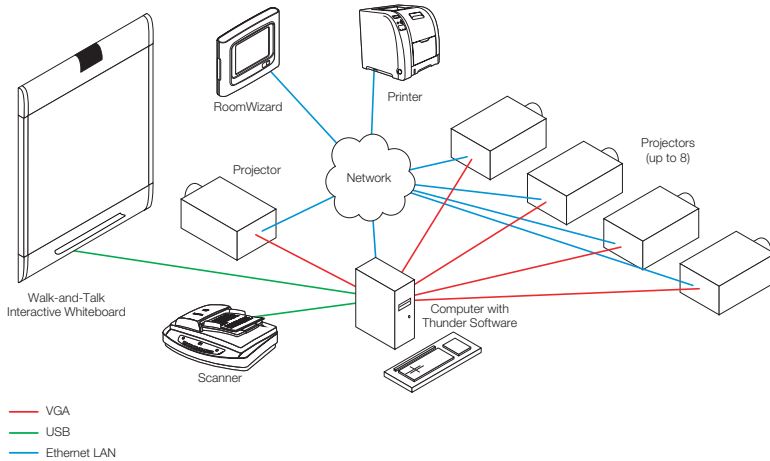
The number and configuration of projectors available to THUNDER Express depends upon the license agreement for that system. THUNDER Express can be used with zero to eight projectors.

In collaborative THUNDER Express environments, one video output is provided to a large interactive input device, such as a projector and interactive whiteboard, interactive LCD, or interactive plasma display, which acts as the easel for the system. Additional projectors can be used for “posting” flipchart pages on the wall to keep them in view as a new page is filled.

In more presentation oriented THUNDER Express environments, projectors may be desirable for posting filled pages on the wall, or they may not be required. For example, a small lecture hall may be equipped with THUNDER Express installed on a desktop computer, an IP17 Interactive Panel at the lectern, and eight projectors for posting pages that the lecturer has already presented, to keep them in view as the lecture proceeds. Alternatively, the same THUNDER Express environment may involve no projectors, but with each participant, whether in the room or connected remotely, joining the session using THUNDER client on their laptop, where they can save the session for later review.

HARDWARE CONNECTIONS

THUNDER Express software expects the main video output from the computer to be connected to a device that displays the virtual flipchart workspace such as the Walk-and-Talk Interactive Whiteboard shown below. Use other video outputs to connect projectors for the display of pages that are “posted” on the wall.



PolyVision can provide a 4-output projector card to add capacity to your system.

NOTE:

Windows Vista requires all video cards to be made by the same manufacturer. To add capacity, you may need to disable the built-in video card.

A

administrator setup pages **26, 45**
 alignment pattern
 projector **41**
 anti-virus software **65**
 Audio
 status **73**

B

bandwidth **53**
 batteries
 stylus **70**
 booting the system **36**

C

client software **60**
 color balance **41**
 configuration options for Thunder **45**
 configuration wizard **37**
 configure and test components **35**

D

default password **46, 54**
 demilitarized zones **18**
 deploying Thunder
 considerations **30**
 Desktop Sharing Serial Key **39**
 Diagnostics **72**
 DMZs **19**
 DVD **44**

E

easel
 cleaning **66**
 rotation **49**
 start software **42**
 Easel setup page **48**
 easel software
 exiting **39**
 updating **62**
 email functions **59**

email server **55**
 Email setup **55**
 exit Thunder software **40**

F

firewall **28**
 connections from inside **32**
 connections from outside **30**
 Flash Communications Server **28**

H

Hardware setup **52**
 hibernation **49, 66**
 home page appearance **47**

I

Internet Explorer **45**
 upgrading **65**
 island networks **15**
 IT system manager **35**

K

key
 Windows XP **37**
 key frame interval **53**

L

LDAP **55**
 LDAP servers **59**
 license number **10, 50, 58**
 licensee name **50, 58**
 Lighting
 status **73**
 localhost **45**

M

monitor
 cleaning **66**

N

network authentication **25**
 network security
 planning **13**

O

One-Click Publishing **11**
 operating system update **25**
 overview **6, 10**
 projectors **10**
 RoomWizard **11**

P

passwords
 administrator **54**
 changing **54**
 for sessions **28**
 for system administration **46**
 user level **27**
 pen
 batteries **70**
 phone
 status **73**
 plasma monitor
 cleaning **66**
 port 1935 **31**
 ports
 used by Thunder **29**
 printer configuration **53**
 private conferences **28**
 projector **10**
 alignment **35**
 alignment pattern **40**
 brightness **51**
 configuration **51**
 configuring **40, 41**
 video card **10**
 projector licensing **10**
 Projector status **73**
 projectors
 sharing **67**
 Projectors setup page **67**
 public access **20**

Q

quality of video **53**

R

RCA **44**

read-only conferences **27**
 Real-time Messaging Protocol (RTMP)
 30

remote access **26**
 room control **71, 72**
 diagnostics **72**
 IP address **54**
 Room setup page **47**
 RoomWizard **11**
 configuration **59**
 rotating the easel **49**

S

scanner resolution **53**
 scanner source ID **53**
 screen savers **25**
 security
 application level **27**
 Security setup page **54**
 serial number **37**
 Windows XP **37**
 sessions
 backing up **65**
 deleting **63**
 setup pages **46**
 shared projectors
 recovering **67**
 SMTP
 server **55**
 usage tracking emails **55**
 software
 exiting **45**
 software updates **62**
 standalone systems **14**
 Status setup page **58**
 stylus
 batteries **70**
 tip replacement **70**
 system
 configuration **39**
 security **24**
 wiring overview **8**

T

three-letter ID **49, 53**

Thunder client software **60, 61**

installing **61**

updating **62**

Thunder Express **5**

hardware configuration strategies
78

overview **9**

projector configurations **79**

system requirements **33, 78**

Thunder Pro **5**

Thunder server

booting **36**

cleaning **66**

equipment configuration **7**

timeout period **49**

tracking usage **56**

troubleshooting **74**

U

Usage setup page **56**

usage status **56, 58**

user-level authentication **25**

V

VCR **44**

video

input **44**

video card **10**

video resolution **53**

video source ID **53**

Virtual Private Networking **17**

W

Windows Vista **80**

Windows XP **24**

accessing on the easel **39, 45**

serial number **37**

wireless keyboard **12, 35**

