MEZZANINE TECHNICAL OVERVIEW

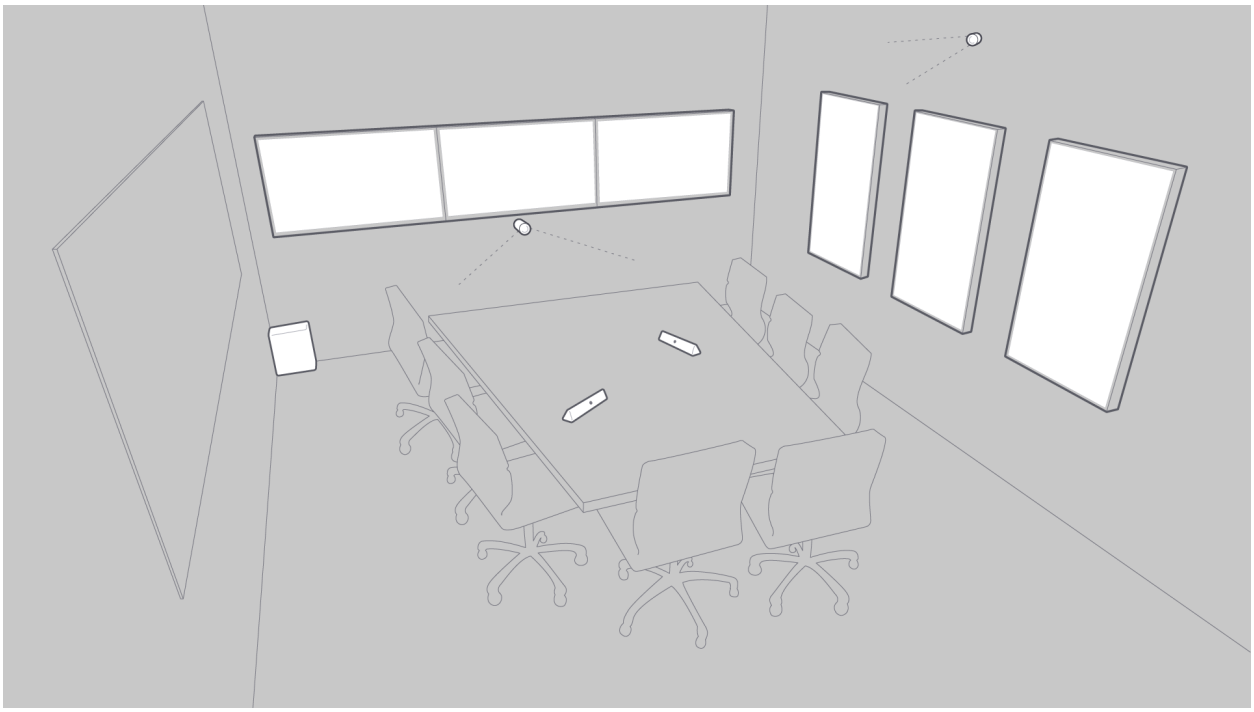
Released: 11 April 2014

TABLE OF CONTENTS

OVERVIEW

What is Mezzanine?

Mezzanine™ is a collaborative conference room solution that introduces multi-user, multi-screen, multi-device collaboration. This is next-generation communication: share any content from any device with anyone, anywhere.



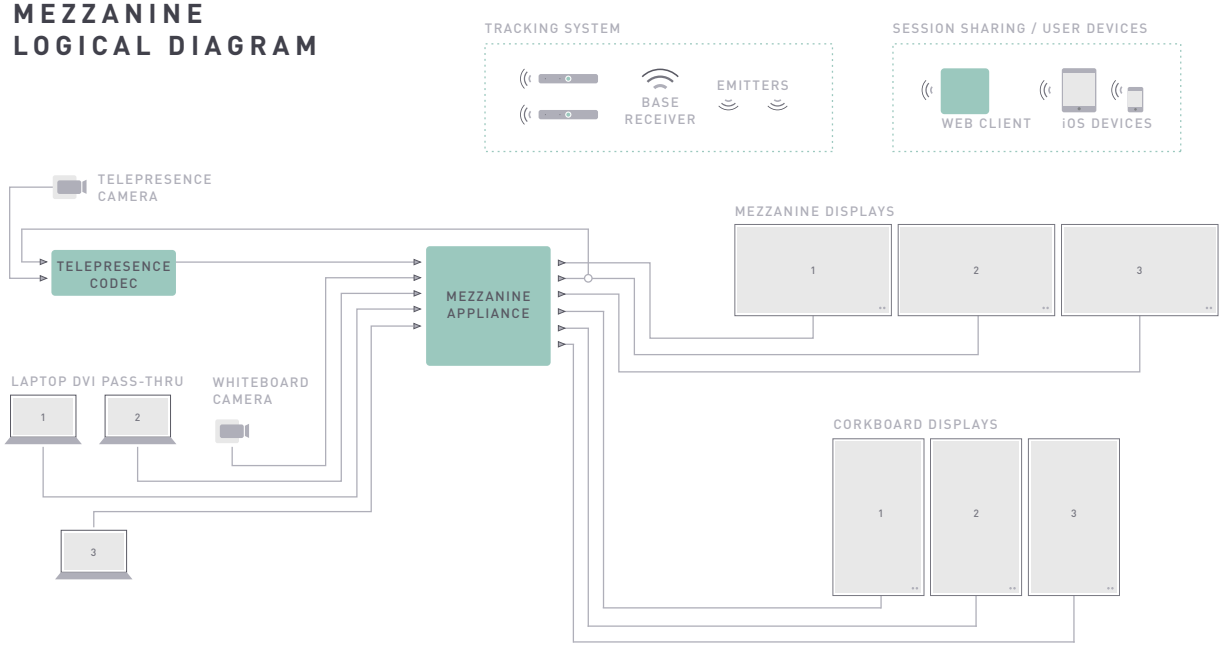
Mezzanine's technology transforms the workspace, allowing for:

- Multiple users to bring their own devices and share content across multiple screens
- Infopresence multi-room connectivity
- Support for web browsers, smartphones, and tablets (iOS and Android supported)
- Presentation control, on-screen content manipulation, and whiteboard capture via the wand — a spatially-aware input device
- Control of connected laptops and their applications in the room via the wand and web browser
- Compatibility with existing videoconferencing infrastructure
- Integration with several screen sizes, from affordable standard LCDs to high-end, edge-blended display walls
- Easy integration with enterprise authentication systems that speak LDAP

All of these capabilities combine to create a hyper-capable, hyper-connected environment. A standard Mezzanine installation comprises the following components:

- Mezzanine appliance running Oblong's proprietary code that drives up to 6 displays
- Whiteboard camera, usually connected to the appliance over a private network
- A tracking system for the spatial wand, communicating with the appliance
- Peripherals for ingesting video from laptops and other devices into Mezzanine
- Various user devices, connected to Mezzanine using Oblong's proprietary software

MEZZANINE LOGICAL DIAGRAM



What are Mezzanine's technical specs?

COMPONENT	DESCRIPTION
Mezzanine Appliance	Dell Precision T5600 + third party hardware
Video Inputs	4 x DVI Inputs Support Formats: 720p50, 720p59.94, 720p60, 1080p23.98, 1080p24, 1080p25, 1080p29.97, 1080p30, 1080i50, 1080i59.94, and 1080i60
Video Outputs	6 x DVI (or digital video equivalent) Supported Format: 1080p60
Network Interface Connections	1 x Network Port 1 x IP Whiteboard Camera
Tracking Interface Connections	1 x Ultrasonic Emitter Port 1 x Radio Receiver Port
Hard Drives	4 x 1 Terabyte drives RAID 10 configuration for redundancy
Operating System	Ubuntu 12.04 LTS
Dimension	4U appliance: 16.30 x 6.79 x 18.54 in
Weight	29.1 lbs
Power	V: 100-240 V A: 6 A Hz: 47-63 Hz W: 825 W
Operating Environment	50°F - 95°F (10°C -35°C)

What are Mezzanine's room requirements?

Conference rooms come in a variety of shapes and sizes. In order to determine which of your rooms are good candidates for Mezzanine, here are characteristics of rooms that are well suited for Mezzanine:

Location

- Class A (business / commercial) facilities
- Indoor environments only
- For secure facilities that prohibit radio frequency use, an optical tracking version of Mezzanine is available; special requirements apply for optical tracking

Room size and characteristics

- Typical room size 15 x 15 to 30 x 30 ft. (4.6 x 4.6 to 9 x 9 meters)
- Ceiling height: 9 - 13 ft. (2.75-4m)
- Maximum tracked area (assuming 13 ft. ceiling): 15 x 25 ft. (4.6 x 7.6m)
- Drop ceiling with standard T-bar and ceiling tile sizes

Appliance location and storage

- Appliance can be deployed either within a credenza in the Mezzanine room or in a nearby server room
- 12U of rack space is required for the Mezzanine appliance and other peripherals, such as video teleconferencing equipment
- Maximum distance from Mezzanine room to appliance location is 50 meters

Power requirements

- At appliance location:
    - For US deployments, one 20A circuit, exposed via a NEMA 5-20R socket or C19 receptacle
    - For European Union deployments, one 16A circuit exposed via an adapted local socket or a C19 receptacle
- In conference room:
    - For US deployments, one 20A circuit, exposed via a NEMA 5-20R socket or C19 receptacle
    - For European Union deployments, one 16A circuit exposed via an adapted local socket or a C19 receptacle
- In the Mezzanine room, power distribution is required at the conference table, screen locations, camera locations, and wand charging stations

HVAC

- At appliance location: 12,000 BTU*
- In conference room: 4,000 BTU*
- When possible, airflow should be limited near the ceiling mounted emitters

**Represents the heat load generated by Mezzanine hardware and peripherals, not accounting for other heat sources, such as lighting, people, and other hardware.*

Preferred lighting

- Indirect lighting around a room's perimeter is preferred for optimal display viewing
- Even lighting over the whiteboard for enhanced image quality

Device interference

- Ultrasonic occupancy sensors must be avoided within the desired room; passive infrared sensors should be used when possible
- Since Mezzanine's tracking system utilizes radio communication at 900MHz, ensure that there is an open channel in the 900MHz range in the desired room
- For European Union deployments, Mezzanine's tracking system will utilize 2.4 GHz radios, where 2 channels are required

Whiteboard recommendations

- Minimal reflectivity is preferred to reduce the glare of displays or lighting
- Non-transparent whiteboard surfaces are preferred in order to provide a high contrast between the whiteboard surface and the marker color

What hardware is included in a Mezzanine bill of materials?

The hardware in a Mezzanine room varies based on the desired use of a Mezzanine system. As a result, different equipment may comprise a Mezzanine room. A standard Mezzanine bill of materials includes:

COMPONENT	MANUFACTURER	PRODUCT	QUANTITY
Mezzanine Appliance	Various	Third-party components	1
Tracking Hardware	Oblong	Ceiling-mounted emitter pods	Up to 36
	Oblong	900 MHz ultrasonic wand*	2
	InterSense	900 MHz receiver*	1
	Oblong	Wand storage case	1

** 2.4 GHz wands and receivers are available for European Union deployments.*

Add-on peripherals may include:

COMPONENT	MANUFACTURER	PRODUCT	QUANTITY
Mezzanine Displays	Various	Sizes ranging from 46" – 75"	3
Corkboard Displays	Various	Sizes ranging from 46" – 75"	Up to 3
Video Teleconferencing	Cisco, Polycom, or LifeSize	Standards based codec	1
Whiteboard Camera	Arecont	IP camera	1
Audio system	Various	Mixer	1
	Various	Amplifier	1
	Various	Speakers	2
Power support	Server Technology	Switched PDU	1

CONNECTIVITY

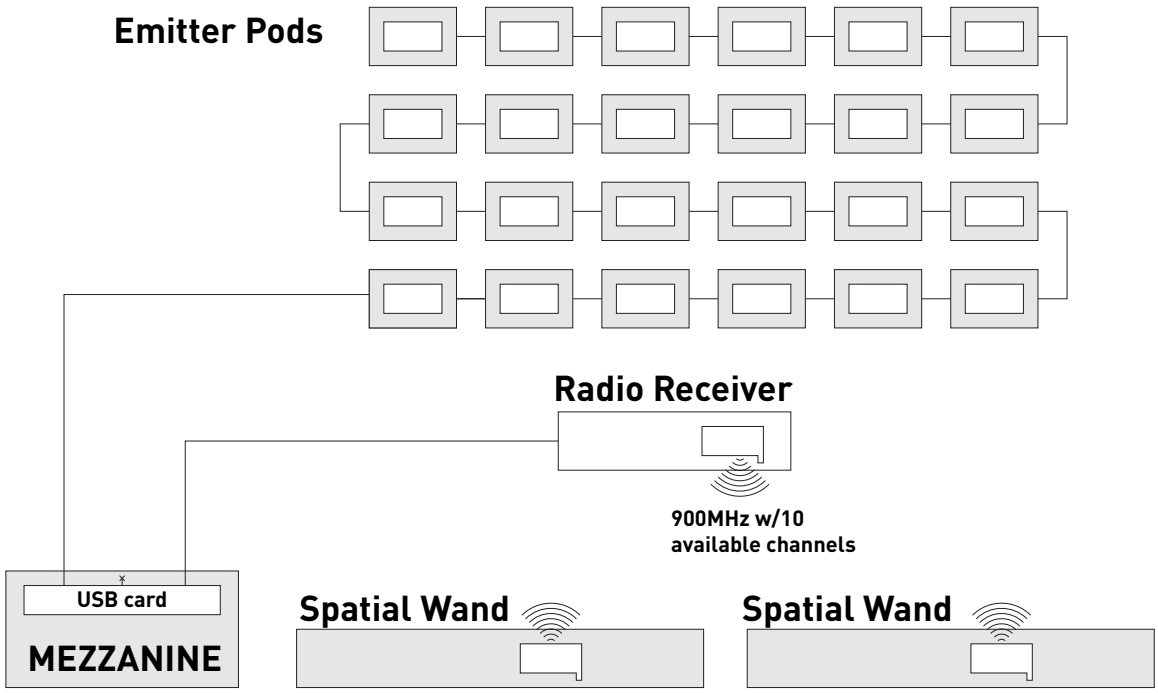
What type of interconnectivity is required for Mezzanine?

Sensors

Mezzanine utilizes an ultrasonic tracking system in order to enable spatial wands to interact with a Mezzanine system. The ultrasonic tracking contains four primary components: spatial wand, ultrasonic emitters, radio receiver, and a USB interface card.

Tracking system overview

Mezzanine comes equipped with two spatial wands, which act as the primary user interface to Mezzanine. These wands communicate with both ultrasonic emitters and a radio receiver to provide Mezzanine with position and orientation information for each spatial wand. This information is used by Mezzanine to enable the wand to act as a pointing device. As a result, a user can point his or her wand at a screen to control content and move that content to any screen within the Mezzanine room.



A closer look: Ultrasonic emitters, radio receivers, and USB interface card

Up to 36 ultrasonic emitters are mounted on the ceiling of a Mezzanine room, enabling tracking for up to a 15' x 25' area. The emitters can be installed in a number of ways: mounted onto a finished ceiling with emitter bars; mounted onto T-bar of drop ceiling with emitter pods; or mounted architecturally into the room where all sensor equipment resides above the ceiling in a plenum area.

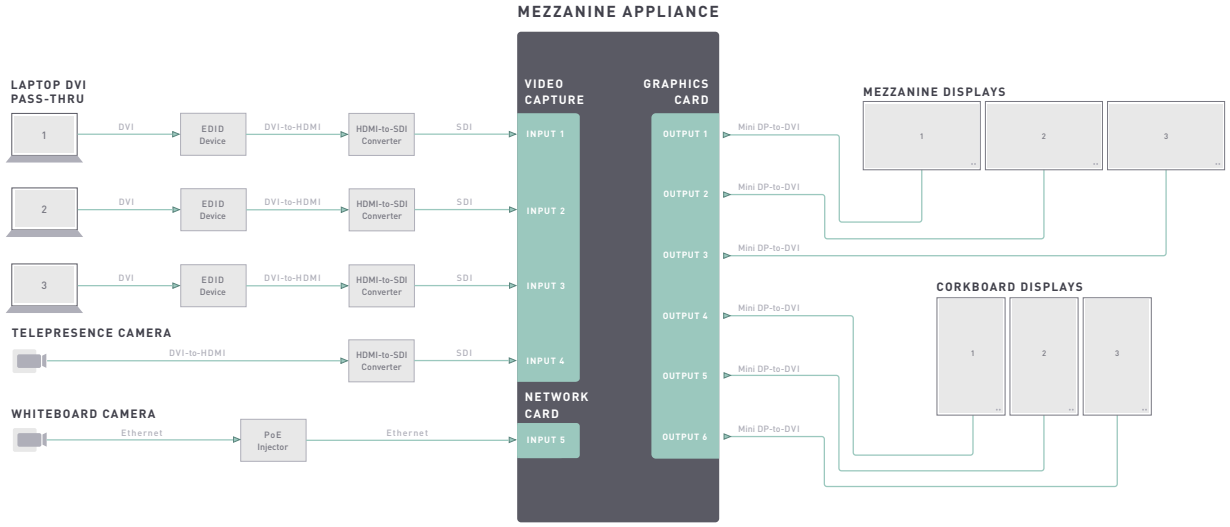
Each Mezzanine room comes with a single radio receiver, which receives position and orientation information from the wand and reports that information back to Mezzanine. The spatial wands and radio receiver communicate with each other via radio frequency at 900MHz (or 2.4 GHz for EU deployments). The tracking system's components are connected to a USB interface card that resides within the Mezzanine appliance. The USB interface card is connected to both the ultrasonic emitters and the radio receiver via 10p10c cables.

Video

A standard Mezzanine appliance is equipped with five video inputs and six video outputs. For video inputs, Mezzanine can accept four HD video feeds from sources that are capable of outputting digital video and one IP video stream from an IP video camera. For video outputs, Mezzanine is capable of driving up to six 1080p displays.

See below for a sample video flow.

MEZZANINE VIDEO FLOW DIAGRAM

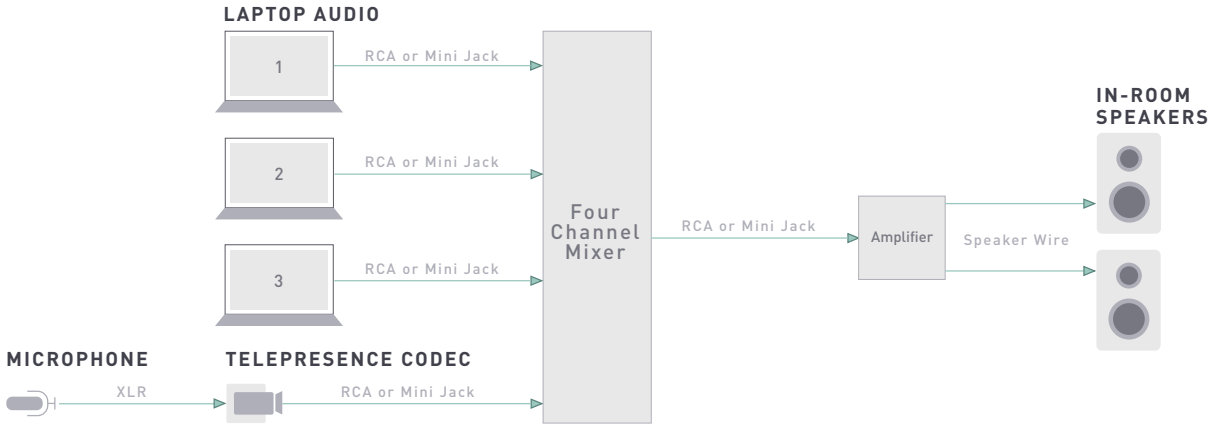


Audio

Mezzanine does not provide native audio support, but Oblong delivers an auxiliary audio solution to supplement Mezzanine and its attached peripherals.

See below for a sample audio flow.

MEZZANINE AUDIO FLOW DIAGRAM



Network

Mezzanine has two network interface cards that are used to connect Mezzanine to: 1) a network port for network connectivity, 2) an IP streamed camera.

For detailed information regarding the network configuration, refer to the Networking section.

NETWORKING

What network configuration is required for a Mezzanine?

For each Mezzanine room, you will need to allocate the Mezzanine appliance with an IP address and a DNS entry. When possible, a static IP address should be used for Mezzanine.

If you are installing multiple Mezzanines that will be connecting to each other, you will need to provide a means for each Mezzanine to route its traffic to other Mezzanines.

What network configurations are recommended to connect multiple Mezzanines?

There are a number of ways that you can configure your network to enable Infopresence communication; here are three options:

- Option 1: Since Mezzanine's protocols are not currently NAT-aware (Network Address Translation), each Mezzanine appliance must be on routable subnets to one another where NAT traversal is not required. The simplest way to accomplish this setup is to use a site-to-site VPN to route the appropriate subnets directly. For this configuration, it is acceptable if each Mezzanine is on a separate subnet, as long as they are all routable.

- Option 2: If an existing WAN is in place – either via a VPN or publicly – through which VLANs are maintained, all Mezzanines could be placed within a single subnet in a single VLAN.

- Option 3: The Mezzanine appliances can be placed directly on the Internet or in a DMZ area of your network. While Mezzanine does provide encryption for data being transmitted over the Internet, this method of connecting is not recommended for various system security reasons. The security reasons are not Mezzanine specific but would fall under best practices for system security.

What are Mezzanine's network Service Level Agreement (SLA) requirements?

For an optimal Infopresence connection, the following network requirements are recommended:

- Bandwidth between each Mezzanine should be at least 15 Mbps for upload and download
- Network latency between each Mezzanine should be no more than 150 ms each way (i.e. 300 ms for round-trip network traffic)
- Peak-to-peak delay variation (jitter) should be less than 10 ms
- Packet loss between each Mezzanine should be less than 0.05%

What if my network doesn't meet Mezzanine's network SLA requirements?

For local Mezzanine sessions, the network SLA requirements do not impact the Mezzanine session. Network SLA requirements apply to Infopresence sessions only.

Mezzanine provides the ability to stream a number of high definition video sources to and from a number

of locations simultaneously. If your available bandwidth is less than the SLA requirement specifies, then fewer full motion videos will be allowed to stream simultaneously between Mezzanines. Specifically, once all available bandwidth has been consumed, the video feed which was accessed least recently will begin to thumbnail – a frame of video will appear every 4 seconds. By forcing videos to thumbnail, the bandwidth on the local network is preserved while allowing some streaming video to continue within Mezzanine.

For most office applications, such as Word, Excel, and PowerPoint, video thumbnailing is minimally disruptive to the end user. If dynamic applications or video is required, then additional bandwidth may be required.

What types of configuration options are available for network streaming?

Mezzanine's web-based admin tool enables a system administrator to configure the amount of bandwidth - both maximum and minimum - for individual video feeds, as well as the overall maximum bandwidth used by Mezzanine.

Based on available bandwidth, these controls allow for Mezzanine to be fine-tuned. On a high performance network with ample bandwidth, Mezzanine can be configured to enable a significant number of high definition videos to be streamed to other Mezzanines. Conversely, for bandwidth limited networks, Mezzanine can be configured to restrict the overall bandwidth consumption to meet the requirements of the network.

How can an Infopresence session's traffic be optimized via QoS?

Mezzanine utilizes RTSP to stream videos between Mezzanines. If a QoS-capable network router or switch is used to manage network traffic, then RTP packets can be prioritized in order to improve the video quality between Mezzanines.

What protocol is used to connect Mezzanines in an Infopresence session?

Mezzanines connect to one another via an Oblong proprietary protocol called MIP (Mezzanine Interconnection Protocol). MIP is responsible for handling collaboration negotiation between Mezzanines, peer discovery of other Mezzanines, and presence notification (i.e. heartbeats) between connected Mezzanines.

How do devices connect to a Mezzanine room?

Laptops and mobile devices can be used for control of Mezzanine, viewing content within Mezzanine, and sharing video feeds into Mezzanine. For these devices to connect to Mezzanine, they need to either be on the same network as Mezzanine or be connected to a network which is routable to the Mezzanine network.

How many Mezzanine rooms can connect in a single session?

Mezzanine allows for up to four rooms to connect and share content simultaneously. When Mezzanine rooms are connected, their content is digitally interlocked, meaning that all Mezzanines are viewing and controlling the same content.

SECURITY

What is Mezzanine's threat model?

At a high level, threats to Mezzanine can be organized along the following attack vectors:

- Physical
- Administrative Interface
- Client Communication
- Infopresence Sessions
- LDAP Communication

A combination of security features built into Mezzanine along with recommendations for mitigating these attack vectors result in creating a secure environment for your Mezzanine appliance. Let's take a deeper look at each attack vector and see how threats can be mitigated.

Physical

ATTACK VECTOR	MITIGATION
Data stored on a Mezzanine can be compromised in cases of theft or tampering.	Mitigate by securing access to the appliance. Further mitigate by configuring Mezzanine, via the administrative interface, to enforce a lifespan on all user data.
Peripherals and the tracking system communicate with Mezzanine over wired connections.	Mitigate by securing access to the facility and by periodically examining equipment for signs of tampering.

Administrative Interface

ATTACK VECTOR	MITIGATION
Brute force attacks against weak passwords.	Mitigate by using strong passwords.

Client Communications

ATTACK VECTOR	MITIGATION
Rogue actor watching traffic in transit for confidential information.	Mitigated by the use of TLS for all connections.
Unauthorized user joins a Mezzanine using one of the client applications.	Mitigated by users in the Mezzanine room enabling the pass-phrase feature.
Rogue Mezzanine forges an authentic Mezzanine.	Mitigated by Mezzanine's insistence on valid and trusted certificates.
Rogue actor reverse engineers the proprietary Mezzanine protocol to connect as a client.	Mitigated partially by the use of TLS connections for all traffic, thus preventing sniffing of protocol packets. Further mitigate by network separation such that access to networks that can access Mezzanine requires authentication.

Infopresence Sessions

ATTACK VECTOR	MITIGATION
Unauthorized calling by genuine, external Mezzanine.	Mitigate via network separation.
Unauthorized calling by rogue external Mezzanines.	Mitigated by Mezzanine's insistence on valid and trusted certificates.
External DoS attacks against Mezzanines.	Mitigate via network separation.
Genuine Mezzanine users unwittingly call rogue Mezzanine.	Mitigated partially by requiring administrative access to add a Mezzanine as a potential collaborator. Mitigated against a man-in-the middle spoofing a real Mezzanine by the insistence on valid and trusted certificates.
MITM manipulates RTCP traffic to manipulate video streams.	Mitigated by the use of SRTP.
MITM sniffs media streams in transit.	Mitigated by the use of SRTP.
Rogue DHCP server on the network when Mezzanine is configured to obtain an IP address via DHCP.	Mitigated by site admins configuring port security and DHCP snooping on their switch connecting Mezzanine to the network.

LDAP Communications

ATTACK VECTOR	MITIGATION
Sniffing credentials from traffic in transit.	Mitigated by Mezzanine's insistence on TLS connections.
Rogue LDAP server on the network spoofing the configured server.	Mitigated by the use of a server certificate manually uploaded via the administration interface.

How does Mezzanine secure network traffic?

Mezzanine is designed to work securely out of the box. All Mezzanine traffic that leaves the private network - to another Mezzanine, a client or an LDAP server - is encrypted using TLS, by default. System administrators can configure Mezzanine to use certificates signed by Oblong or purchase and upload third-party certificates. 4096-bit keys and strong cipher suites such as AES (256-bit) and ECDH are preferred everywhere, and null cipher downgrades are prohibited.

System administrators can further control risk through any of the standard network separation techniques that limit which users and services are allowed to access a Mezzanine. For instance, only users on local Wi-Fi or Ethernet networks and a list of known collaborating Mezzanines need access in most situations.

What ports does Mezzanine use to communicate?

Mezzanine only needs a few specific ports to be open (see table below). System admins can safely filter all other traffic.

Mezzanine Required Ports

PORT(S)	PROTOCOL	APPLICATION
80	TCP / HTTP	HTTP redirects to 443 / HTTPS
389	TCP	LDAP admin app
443	TCP / HTTPS	For client access and Infopresence sessions
636	TCP	LDAP secured by TLS
8554	TCP	RTSP control interface
20000-20050	UDP/SRTP	Video streaming ports
65456	TCPS	Plasma communication

How can users keep their information private?

Mezzanine can be connected to an LDAP or Active Directory server to allow users to login to their Mezzanine and store their information privately under their LDAP or Active Directory credentials.

In addition to storing information privately, users can initiate a "locked" session where only participants with the session's passkey can view the content that Mezzanine makes available to web browsers and mobile devices.

How does Mezzanine connect to an LDAP or Active Directory server?

When authenticating against an external LDAP or Active Directory server, the user submitted credentials are not stored on Mezzanine. When a user logs into Mezzanine's web browser app or mobile app, he or she submits a username and password to Mezzanine over HTTPS. Mezzanine then composes an LDAP query with the username and password and sends that query to an external LDAP server. Mezzanine receives a response from the LDAP server, stating whether the username and password combination was either correct or incorrect. With approved access from the external LDAP server, a user can access his or her data stored on Mezzanine.

Alternatively, Mezzanine offers a local LDAP server, which resides on the Mezzanine appliance. In this case, user credentials are stored in an industry standard encrypted format by the local LDAP server. The local LDAP server option enables user accounts to be created by a system administrator in a case-by-case basis for each Mezzanine.

MAINTENANCE

What daily maintenance is required for Mezzanine?

The Mezzanine appliance does not require any daily maintenance. The software and appliance are both designed for always on, 24/7 operations.

In-room devices, such as spatial wands and mobile devices, require daily charging to ensure the devices have sufficient power for the following workday. The wands are designed to run for an entire business day. They contain rechargeable batteries that last up to 10 hours when fully charged. In addition, the wands have a battery preservation feature, which powers off the wands after 30 minutes of inactivity.

If power reduction initiatives are in place at your organization, the displays may be required to be powered on / off on a daily basis.

What periodic maintenance is required for Mezzanine?

Similar to daily maintenance, the Mezzanine appliance does not require any periodic maintenance. If required, Mezzanine has a web-based admin tool that provides a system administrator the ability to restart the appliance or individual processes.

If anomalous behavior is occurring with your Mezzanine, file a support request by emailing support@oblong.com.

Oblong is always looking to improve the Mezzanine experience. If you would like to help us provide a better Mezzanine experience for your coworkers, you can export usage logs from the web-based admin tool and email them to Oblong at mezz-usage@oblong.com.

How are software upgrades provided?

If your Mezzanine is covered by an active maintenance contract, you will receive Mezzanine software upgrades as they become available. Nominally, 2-3 software releases are available per year; these releases include additional features, performance improvements, and bug fixes. A Mezzanine Technical Account Manager will arrive on-site to perform software upgrades when they become available.

See the Support section for more information about the Technical Account Manager and Oblong's support program.

Are security patches available?

Yes, Oblong will release security patches for critical operating system vulnerabilities. Patches will be made available within a reasonable amount of time following the discovery and resolution of vulnerabilities. Your Mezzanine Technical Account Manager will be responsible for patching vulnerabilities.

See the Support section for more information about the Technical Account Manager and Oblong's support program.

SUPPORT

What type of support is included in a Mezzanine maintenance contract?

An active maintenance contract provides you with the following support items:

- Software updates, as they become available
- Assistance through the Oblong Support Portal with respect to the use of the software and hardware, including:
    - Clarification of functions and features of the software and hardware
    - User and administrator documentation
    - Guidance in the operation of the software and hardware
- Error verification, analysis, and correction

In addition, Oblong will provide you with a Technical Account Manager. This individual is focused on helping you make effective use of your Mezzanine by:

- Providing user and admin training
- Consulting on use case best practices
- Installing software updates
- Collecting product feedback

Where can I find more information about Mezzanine support?

Additional support information is available; please contact your Oblong Account Executive, Sales Engineer, or Technical Account Manager.

ROLLOUT CHECKLIST

To prepare for your upcoming Mezzanine deployment, the following list contains items that are normally performed between the date of purchase and the first day the system will be available for use:

- ☐ Oblong performs a final site survey to assess site readiness
- ☐ Oblong provides room modification recommendations, if required
- ☐ If room modifications are required, your company performs any required room enhancements
- ☐ Your company configures your network for Mezzanine, including local IP addresses and DNS entries for each Mezzanine and network connectivity for Infopresence connections
- ☐ Your company gathers LDAP or Active Directory server information required to connect Mezzanine to your company's LDAP or Active Directory servers.
- ☐ Oblong performs the Mezzanine installation, normally 4-5 days in length
- ☐ Oblong provides training for your IT staff and end users

