



# GlobalMeet Secure Meetings

December, 2010



ENERGIZE YOUR CONNECTIONS™





## Introduction

GlobalMeet is a hosted web conferencing service intended to deliver enhanced productivity in all meetings. The service offers users the ability to share, present or collaborate on information and documents, take polls, chat privately or with the group, brainstorm on a whiteboard or hold a formal question and answer session and much more. GlobalMeet provides users with all the tools they need to hold an effective meeting with users in the room or around the world.

The product has been designed with high regard for the security of our clients and their data. PGI has a long history of strong security and of successfully safeguarding our clients. GlobalMeet is continuing that tradition today and the company continues to invest in the technology and human resources required to stay at the forefront of security.

This white paper covers the security specific to the GlobalMeet product and should be seen as an addendum to the Premiere Global Resilience, Security and Continuity Resources whitepaper that covers PGI Meet security from a broader perspective.

GlobalMeet Security can be broken out into the following categories:

- > Access Controls
- > Application Security
- > GlobalMeet Architecture
- > Data Security
- > Physical Security

## Access Controls

Access controls provide the initial layer of security for the GlobalMeet product. Moderator functions such as meeting scheduling, room creation, content uploading and the actual initiation of a meeting all require authentication as a PGI moderator with an assigned Meeting Hub (hub) and the moderator's company must have access to the GlobalMeet product.

**Moderator Authentication.** In PGI parlance the “moderator” is the account owner. The moderator is empowered to create conferences and schedule meetings within their own account. The PGI authentication model for moderators consists of a client account with a client ID and web password pair. These credentials are assigned during account creation by one of the account provisioning systems. The client ID is a 7 digit numeric that remains static throughout the life of the account. The password policy is customizable on a company by company basis; if no customization is requested new accounts for that company will follow the default password policy. The default is a randomized string consisting of 4 alpha characters and 2 numerics. Once the client logs in with the default password they will be prompted to change their password to a user defined password that must match the client company's password policy.

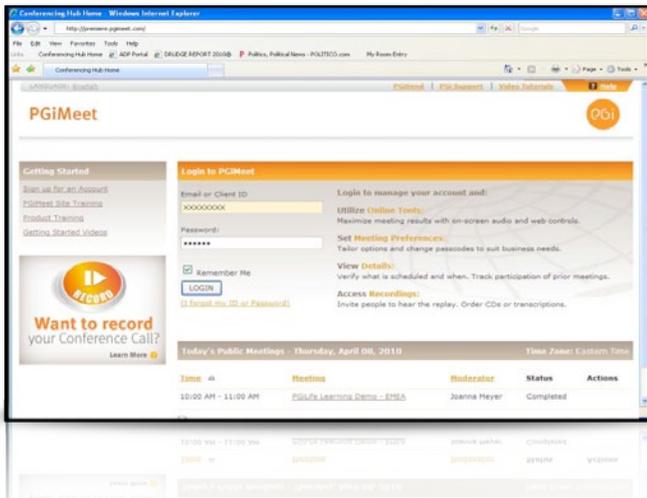
The possible customizations to a company's password policy are:

- > Number of days before password expiration.
- > Number of days for a grace period for this password expiration
- > Password expires upon first login
- > Number of alpha characters that must be in the password
- > Number of numeric characters that must be in the password
- > Number of special characters that must be in the password
- > Minimum length of a password
- > Maximum length of a password
- > Default password for new client accounts (if desired)

This model of default with optional customizations provides for a high level of flexibility for our clients to define their authentication model from medium to high security.

In addition to options related to creation and management of credentials, all failed login attempts are logged for reporting and analysis should the need arise. PGI's Technical Operations team constantly reviews system behaviors and logs for unexpected trends or unwanted behaviors.

**Meeting Hub Assignment.** PGI provides its customers a single portal for all of their collaboration needs. The Meeting Hub (Hub) provides users access to account management tools, audio conference management tools and access to our web conferencing tools including GlobalMeet. The assignment of a new client to a Meeting Hub is handled by a proprietary application accessible only on the PGI network by a select group of PGI personnel. Access to this application is based on a systemic role which follows the "least privilege" PGI policy.



The customer can designate one or more site administrators for a given Meeting Hub. This Meeting Hub administrator will serve as the client side controller of accounts and rights in the Meeting Hub. If a company elects to segment their user base into multiple Meeting Hubs a Hub Group Administrator can be created. The Hub Group Administrator can perform all normal administrative functions with the addition of the ability to designate hub admins and manage users across the Meeting Hubs under their control.

There are two additional layers of administrative roles for the Meeting Hub: the Provider Administrator which is primarily used by our resellers to manage their customers, and the Global

Administrator which is a role held exclusively within PGI for purposes of troubleshooting and problem resolution.

**GlobalMeet Access.** The final layer of access control for moderators is a company's decision to grant access to the GlobalMeet product within their Meeting Hub. Access to any PGI product from within the Meeting Hub can be enabled or disabled. The Meeting Hub administrator does not have the ability to enable/disable these services; it must be done by a PGI employee with sufficient privileges within a proprietary application accessible only from the PGI network or by an authorized reseller Provider Administrator. The ability to prevent access to services allows PGI clients the certainty that they will not incur charges for non-approved services or from approved services but non-approved employees.

The three levels of access controls required for moderators to schedule, create rooms and conferences or access content involve both systemic and human steps and provide a substantive barrier to unauthorized access to the GlobalMeet service.

## Application Security

Access controls focus on the prevention of unauthorized access to the service as a moderator. Ensuring that no unauthorized attendees are allowed into a meeting requires an additional layer of features and functions. GlobalMeet offers moderators a robust security model to prevent unwanted attendees in their meetings.

**Meeting Roles.** The GlobalMeet product uses roles to separate features and rights in the meeting between the account holder and the attendees.

**Moderator.** The Moderator of the meeting is the account holder. As such they are granted the highest level of control of the meeting and are the only meeting participant that has access to promote others to co-presenter status or initiate recordings. Moderator controls include:

- > Application Sharing
- > Share a presentation
- > Whiteboard
- > Q&A
- > Upload content
- > Polling
- > Lock
- > Record
- > Full-screen
- > Promote to co-star



- > Share files for download
- > Invite others
- > Dismiss others
- > Audio controls
- > Webcam video

**Co-Star.** The Co-star is granted a level of rights similar to that of a moderator with the exception of the promoting others to the Co-star role or initiating a recording.

**Attendee.** The Attendee role is the most limited. Attendees have the ability to view a presentation, participate in polls, chat and Q&A, control their own audio and download files if granted permission by the moderator or view and update the whiteboard based on rights provided by the moderator.

These roles segment control of the meeting and provide a level of protection to moderators and companies from unwanted participants or unintended access to corporate documents and information.

**Meeting Options.** GlobalMeet meetings offer users a number of options during meeting setup that provide added layers of security. Many meeting options are also impacted by the selections of a Meeting Hub administrator in the Meeting Hub management pages.

**Scheduled or On-Demand Meetings.** GlobalMeet offers moderators the ability to schedule a one-time meeting with a unique URL or elect to create an on-demand, always available meeting room with a persistent URL.

A scheduled meeting uses a one-time meeting URL. The URL delivered to participants consists of the GlobalMeet URL and a unique GUID that references the true meeting URL housed in the GlobalMeet database. The delivered URL is trapped by the Meeting Hub server infrastructure which in turn looks up the true meeting URL.

<http://url.pgimeet.com/go/?k=70529c21f0d94e39815ccfccee1ffb5b>

While the GUID will remain an active link to the meeting join page, the true URL for the meeting will expire at the scheduled meeting end time, preventing re-use or misuse of past meeting URLs.

On-demand URLs provide access to persistent, always available meetings. These user-definable URLs consist of the address of the company's Meeting Hub and a user-defined extension for ease of meeting entry.

<http://{company.Meeting Hub.name}.pgimeet.com/web/{roomname}>

The availability of a persistent URL implies some inherent risks but these risks can be well managed with other features in the product.

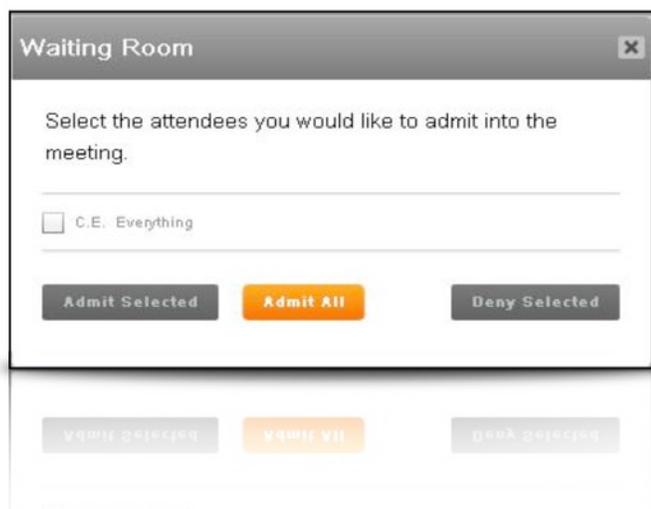
**Public or Private Meetings.** The GlobalMeet application allows users to create meetings as either public or private. Public meetings are listed on the login page of the Meeting Hub and are essentially open meetings to anyone. Setting a meeting as public would be appropriate in instances of a public demonstration of a product, a public seminar or other meetings where no proprietary information will be shared. Moderators are ultimately responsible to set their meetings appropriately but the Meeting Hub Administrator can set the default to private meetings for all users.

Private meetings are not published in the meetings list on the login page of a Meeting Hub, but are listed for the meeting owner in the meetings list viewed after logging into the moderator's Meeting Hub. Both scheduled and on-demand meetings can be set as private. Attendees can only access private meetings via an invitation to the meeting or via the users' defined URLs.

**Attendee join options.** For on-demand meetings the moderator can choose from three methods to manage attendees joining their meetings.

- > **Option 1,** Attendee can join before the moderator, essentially leaves the meeting room open to anyone at anytime. This method is not recommended as a best practice. These attendees will not be able to access content but their time in the meeting room will be charged at the customer's per minute rate.
- > **Option 2,** "Allow attendee to enter only after Moderator" prevents attendees joining the meeting room without the presence of the moderator. This offers a higher level of security and prevention of unnecessary charges. In this scenario an attendee attempting to join the conference without a moderator presence is notified that they will be put into the meeting once a moderator joins. If the moderator doesn't join the meeting for 15 minutes the attendee will be asked to attempt to rejoin within 15 minutes of a moderator joining.
- > **Option 3,** Moderator must admit attendee, offers the highest level of security and prevention of unwanted

charges. In this scenario the attendee attempts to join a meeting and will be placed in the waiting room. The moderator is notified that someone is in the waiting room and asked to approve or deny each request for entry. This option should be seen as the best practice for meeting entry for enterprises with security concerns.



**Post Conference Reports.** To provide moderators detailed information to track the usage of their account, GlobalMeet and the Meeting Hub offer several types of reports.

**Meeting Logs.** At the conclusion of each GlobalMeet meeting the moderator is given the opportunity to view a log file of the meeting. The logs include listings of each attendee joining or leaving the meeting, content shared including slide by slide changes, polling questions, submitted and answered questions, start and stop of application sharing, and the use of most other features. Log files are also accessible for any meeting held in the last 180 days via the Meeting Hub.

**Completed Meetings reports.** A higher level of report is also available through the Meeting Hub. The Completed Meetings report lists all GlobalMeet or audio only meetings held in the last 180 days. This report provides users and administrators an easy view of the activity on their accounts to view any aberrant behavior or trends.

**Meeting Hub Options.** In addition to meeting options manageable by meeting moderators, there are a number of options at the Meeting Hub level intended to allow companies to define policies that suit their situation and enforce them with self-service controls. These controls are not granted

to moderators but only to Meeting Hub administrators. The first administrator on a Meeting Hub can only be created by an authorized PGI employee with access to our proprietary customer support platform or by an authorized reseller provider administrator.

There are two levels of administrator that can be created. Meeting Hub Administrators have control over the specific Meeting Hub to which they are assigned and have the following capabilities:

- > Meeting Hub branding: site logo, site color scheme, support contacts list, account sign up link behavior
- > Meeting Hub settings: GlobalMeet options, site time-zone, default conf title, etc.
- > Create, edit, delete moderator accounts
- > View, edit or delete any moderator's conference, recording or GlobalMeet content
- > View/export usage reporting for all moderators
- > View/export a detailed moderator report

Meeting Hub Group Administrators have all of the capabilities of an Administrator but they can administer any Meeting Hub in the group and create Meeting Hub administrators in any Meeting Hub in that group. For a complete description of the Meeting Hub structure please contact your PGI Sales representative.

The features listed below are available to a Meeting Hub moderator or higher. This list only covers a selection of the controls that directly impact security of meetings.

**Conference private by default.** The default setting for all conferences is set to only be visible if a moderator has signed into the Meeting Hub.

**Audio alert when someone joins.** Sets the default for web conferences to play a tone when someone joins a conference.

**Enable call my phone feature.** Allow moderators and attendees to use GlobalMeet to dial to their phones when joining the audio portion of a conference.

**All presentations available.** All presentations to be available to all conferences (including Meet Now conferences) run from the Meeting Hub, as long as the moderator scheduling the conference has been given permission to view the presentation.

**All polling questions available.** All polling questions to be available to all moderators in all of their conferences, as long as the moderator scheduling the conference has been given permission to use the polling questions.

**Allow Web Recording.** Enables the Record button on the live conference toolbar to be used by the conference presenter to create a recording of the Web conference.

**Application Share.** Enables moderators to share different applications from their computers during the meeting.

**Prohibit users from sharing their entire desktop.** Prohibit the sharing of the entire desktop by a presenter to attendees.

**File Transfer.** Enables the presenter to share files for download by attendees during a meeting.

The next network layer is the perimeter network or “DMZ”. This logical sub-network is used to contain the outwardly accessible portions of the GlobalMeet architecture. Traffic in the DMZ is managed by redundant load balancers. The load balancers are programmable layer 7 network switches used to distribute network traffic across the available servers. The load balancers provide all load balancing services for the Java Meeting Servers, Flash Media Servers and Meeting Hub. Our meeting servers and Flash Media Servers both provide portions of the meeting but are not responsible for storing meeting content or meeting data.

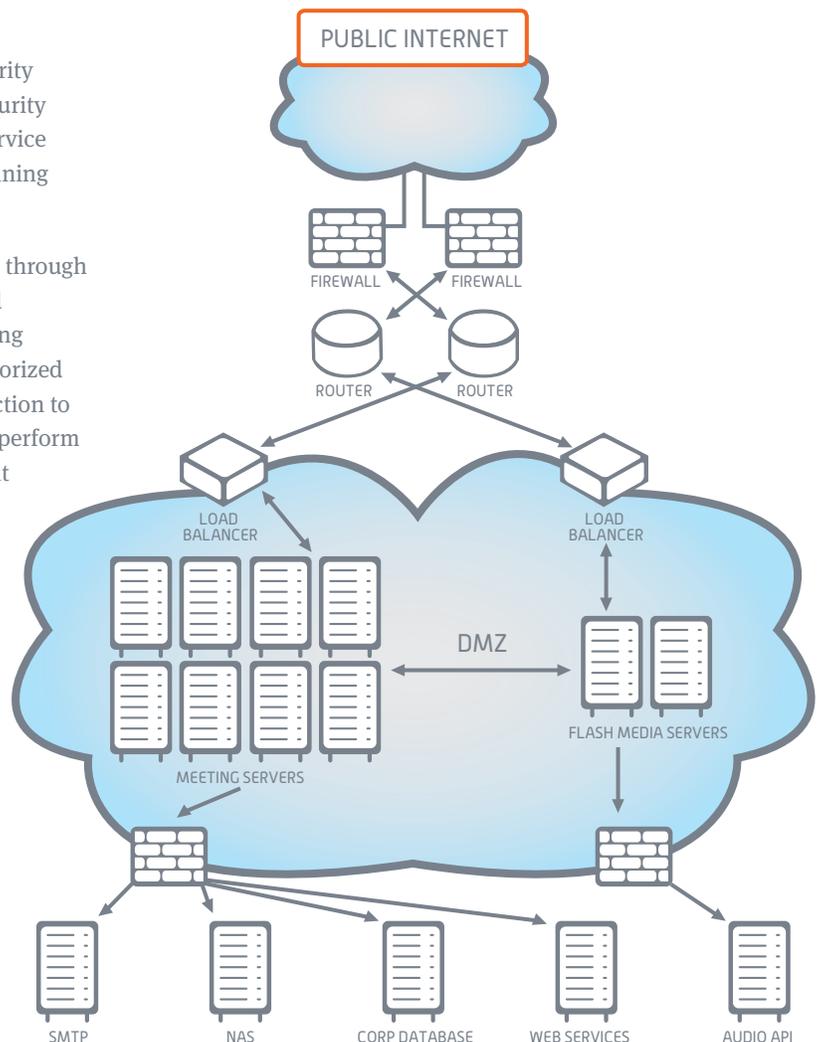
The meeting servers and FMS servers must traverse from the DMZ to the corporate network to retrieve meeting data, meeting content and client information. Entry to the corporate network occurs through an additional set of firewalls to further protect sensitive data and systems.

## GlobalMeet Architecture

The GlobalMeet architecture has been built around security industry best practices and standards as well as PGI Security requirements. The structure ensures that the meeting service remains stable and available to customers while maintaining security for meeting data and content.

Both participants and moderators connect to the service through redundant firewalls and routers. The Firewalls are tuned to permit traffic only on specific ports required for meeting communications using acceptable protocols and to authorized destination IPs. The firewalls also perform packet inspection to prevent spoofed content from entering the network and perform heuristic analysis of incoming traffic looking for aberrant behavior or traffic trends.

The routers serve a filtering role in the architecture and prevent communication with non-addressable IPs. This simple control point prevents the still prevalent spider and bot attacks searching for vulnerable servers.





## Data Security

PGI offers clients a high degree of data transmission security when using the GlobalMeet service, the Meeting Hub or any of the other services. Our data security model includes firewall transversal and transmission encryption and data storage security.

**Firewall Transversal/transmission encryption.** The GlobalMeet product uses techniques for data transmission intended to allow our users to leave their firewall intact. PGI understands the needs of our customers to avoid “punching holes” in their firewall to maintain the highest level of network security for their business. To that end GlobalMeet follows a cascading port approach. For all moderator and attendee traffic other than application sharing, a standard RTMP connection via port 1935, the standard port for Flash traffic, is attempted. If 1935 is unavailable the service will attempt a connection via port 80 the standard port for HTML traffic and failing that will resort to a connection port 443. Application share data for attendees is handled in a similar manner. Application sharing data for moderators attempts a direct socket connection via ports 9080, 1270 or 8057. If all three fail the application will attempt an encrypted connection via 443 then 80.

There is an option for a PGI customer that provides an added level of security to their Meeting Hub and GlobalMeet meetings. Secure Conference changes the manner in which firewall transversal is handled by sending all traffic encrypted with 128-bit AES SSL and only on port 443. If either a moderator or an attendee cannot communicate on port 443 then they will be unable to attend the meeting. Under this scenario all transmission from the PGI network to the moderator and attendee networks is encrypted. Once traffic reaches the F5 switch at the network perimeter PGI uses SSL termination to improve performance.

While this does add to the overall security of the meeting there is a corresponding usability impact in latency and the inability of some to attend meetings. Caution should be used when selecting this option.

**Data Storage Security.** Data related to GlobalMeet meetings falls into two categories: meeting data and meeting content. Meeting data which consists of all the metrics of the meeting (attendees, duration, date/time etc), and meeting content consists of all of the PowerPoint presentations and other documents stored in the content library.

Meeting data is served up by the Meeting Hub as meeting logs or summary reports. This information is stored in an externally

un-addressable database. Meeting data is stored online for 180 days and then moved to off-site storage and purged from production systems. As with all corporate data repositories at PGI we follow “least privilege” rules and this data is only accessible by a subset of our Conferencing Network group. For more information on our network policies, data access policies and human resource policies please see the PGI Resiliency, Security and Continuity white paper.

Meeting Content is made up of all documents uploaded by moderators in the process of holding their meetings. Files uploaded to the moderator’s content library are accessible by the moderator until deleted by the moderator or the Meeting Hub administrator. Content is uploaded by authenticated moderators through either the Meeting Hub or the GlobalMeet meeting room and is scanned for viruses or other malicious software immediately upon completion of the upload.

PowerPoint files are converted to Flash files (SWF) immediately upon completion of the virus scan and stored, along with the original PPT file and an XML file containing meta data, in a randomly named separate and distinct directory on our network addressable storage device (NAS). The NAS is the core of meeting content storage. The NAS is externally un-addressable and requires an authenticated moderator to access it through the Meeting Hub or the GlobalMeet meeting room. Non-PowerPoint files are stored in their own randomly named directories along with an XML file containing meta data.

The XML meta data files stored with each file links the file back to the moderator that uploaded it and the list of other moderators the up-loader has shared that file with. If a person is not on that list, editable only by the moderator or the Meeting Hub administrator, then they will not be aware of the file in any way.

When a moderator deletes the file in the Meeting Hub the file, original PPT (if applicable) and the meta data file are purged from the NAS.

Attendees to meetings will receive streamed data for presentations and application sharing but nothing is stored on the attendee’s machine at any time, reducing the risk of data leakage.

As a final note on meeting content, application sharing creates no storable data other than a record of the launch and ending of app share in the meeting logs. No evidence of what was shared exists in the GlobalMeet architecture.



## Physical Security

The GlobalMeet footprint is hosted in a carrier-class facility near our Colorado Springs, Colorado facility. The building offers on-site security personnel and patrols in addition to registered card-key access.

Over and above building security the PGI facility has physical safeguards including a secured, video-taped, card key accessible man-trap for both ingress and egress and heat and motion detection for intrusion prevention. Recordings from the camera system are uploaded to multiple offsite, read-only access servers while simultaneously sending email & pager notification of facilities access to security personnel.

Access to the data center is limited to authenticated personnel following PGI's "least privileged" standard; only a subset of our security and network operations teams are permitted access.

## Conclusion

The GlobalMeet solution is built with the security of our users and their data in mind. The network, hardware, software, personnel and facilities are all optimized to protect the integrity of meetings.

Companies around the world use GlobalMeet daily to meet and collaborate. These users expect their data and meetings to remain secure. PGI recognizes that expectation and works to fulfill our commitment to our clients every day.

## Learn More

Contact us today or visit our website to view customer videos or product demonstrations and get the details on all of our solutions.

## About us

The world collaborates with PGI. Our advanced meeting, conferencing and collaboration solutions energize people and organizations to connect more meaningfully and work together more productively. PGI is headquartered in Atlanta, Georgia with operations in 24 countries worldwide. You can learn more at [www.pgi.com](http://www.pgi.com).

The Terminus Building  
3280 Peachtree Road NW  
Suite 1000  
Atlanta, GA 30305-2422  
tel 404-262-8000  
fax 404-262-8888  
[info@pgi.com](mailto:info@pgi.com)

[pgi.com](http://pgi.com)

