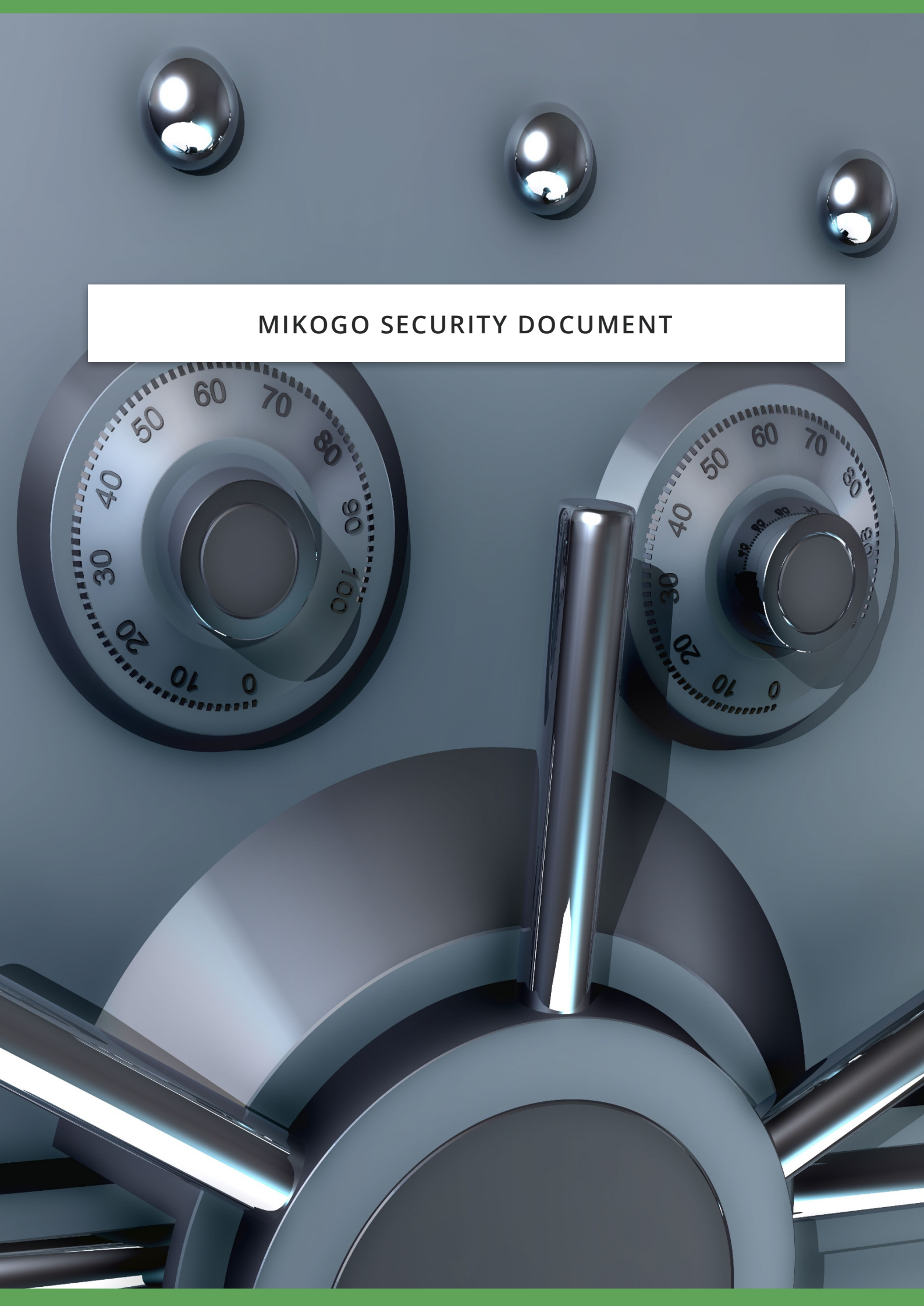
# MIKOGO SECURITY DOCUMENT



## Table of Contents

# The Most Important Facts in a Nutshell

| Content Security | |
|---|---|
| **Data Compression and Encryption** | All content that is shared with the participant in the meeting is compressed with proprietary compression algorithms. This compressed content can be interpreted only by the appropriate Mikogo participant software. Moreover, Mikogo never sends meeting content in clear text, but encrypts all data using 256-bit AES encryption. |
| **Website Encryption** | The Mikogo website is secured with 128-bit encryption using Secure Sockets Layer (SSL), which is the most widely used Internet standard for securing sensitive web data communications. SSL web server certificates are provided and signed by VeriSign/Thawte. |
| **User Interface Security** | |
| **Session ID and Session Password** | A randomly generated 9-digit session ID is assigned to the session organizer to uniquely identify the session. A session password can be defined for additional security. Sessions can only be joined with the session ID and the session password if any. |
| **Roles and Responsibilities** | There are several roles in a Mikogo session: organizer, presenter and participant. The organizer needs a username and password and is the only user who can start sessions. The presenter has the capability to share data. The presenter determines what is shared in a session and the level of access that the participant will have during a session. The presentation rights can be handed over. Before becoming the presenter, the participant has to explicitly agree to transmit their computer screen. These same explicit agreements are also made when granting remote control rights. It is not possible to view or control the computer screen without the explicit consent of the presenter. |
| **Infrastructure Security** | |
| **Third Party Access Prevention** | We employ state of the art firewalls, network monitoring, and intrusion detection tools. Strict change management is employed and additional internal security policies and procedures are enforced. |
| **No Session Data is stored** | Dynamic session content displayed during a Mikogo session originates only from the presenter's machine. The participant sees only representations of this data. At the conclusion of a session, all such representations dissipate. |

## In Detail

Provided by the global online collaboration solutions provider Snapview, Mikogo is an innovative desktop sharing tool used for sales, marketing, training, project management and customer support. Snapview endeavors that the Mikogo services meet the most stringent corporate security requirements. Mikogo assigns data security the highest priority in the design, deployment and maintenance of its network, platform and services. The purpose of this document is to provide information on the data security features and functions that are available in Mikogo and inherent in the underlying communication infrastructure. We discuss the following items in this document: application, firewall compatibility, content security, user interface security, and infrastructure security.

## Application

The Mikogo software communicates with the Mikogo servers located in North America and Europe using proprietary protocols and data exchange methods. It is impossible to participate in a Mikogo session without the close coordination between the Mikogo software and the Mikogo servers. The data in a Mikogo session is shared using the software, which must establish a connection with a Mikogo server. These security features are inherent throughout the session. Each session is dynamic and involves a handshake between the Mikogo software and the Mikogo server, and the communication between these components is by default compressed, encoded, and encrypted.

## Firewall Compatibility

The Mikogo software communicates with the Mikogo servers to establish a reliable and secure connection. When a session is started, the Mikogo software determines the best method for communication. The Mikogo software connects to the Mikogo servers using TCP or http/https protocols over port 80 or 443. In case TCP connections are blocked, the Mikogo software will tunnel all communications using http/https. Regardless of the type of connection that is established when the session is started, firewalls do not have to be specially configured to enable Mikogo sessions.

## Content Security

Mikogo provides several controls to prevent unwittingly sharing data during a session. The presenter can hide the screen at any time to browse through their own confidential files. The presenter can also hide the desktop's wallpaper, the desktop contents, and the taskbar.

### Data Compression and Encryption

All content that a presenter shares with the participant in a session is only a representation of the original data. In addition, all content that is shared with the participant in the session is compressed with proprietary compression algorithms. This compressed content can be interpreted only by the appropriate Mikogo connection software. Moreover, Mikogo never sends session content in clear text, but encrypts all data using 256-bit AES encryption (Advanced Encryption Standard).

### Website SSL Encryption

Mikogo secures its website with 128-bit encryption using Secure Sockets Layer (SSL), which is the most widely used Internet standard for securing sensitive web data communications. SSL web server certificates are provided and signed by VeriSign/Thawte.

### Digitally Signed Software

All software components provided by Mikogo are digitally signed using VeriSign/Thawte certificates, the leading certificate authority.

## User Interface Security

Mikogo security is also enforced through a variety of mechanisms exposed through the Mikogo user interface. The available options depend on the role a session participant assumes.

### Roles and Responsibilities

There are several roles in a Mikogo session: organizer, presenter and participant. The organizer needs a username and password and is the only user who can start sessions. The participant can participate in a session. Both, organizer and participant can become presenter and show their screens.

### Session Parameters

The organizer can specify a 9-digit session ID or use a randomly generated 9-digit session ID to uniquely identify the session. A session password can be defined for additional security. Sessions can be joined by either entering the session ID manually or by clicking on the join session URL in an email invitation or instant message. In either case, it is recommended that the organizer explicitly informs the participant of the existence of the session either by phone or by email.

### Organizer, Presenter and Participant Privileges

Only an organizer can start a Mikogo session using a unique username and strong password. The organizer has the first level of control in the session. The viewing direction can be switched by both the organizer and the respective presenter at any time during a Mikogo session and requires the explicit consent of the participant. The presenter has the capability to share data. The presenter determines what is shared in a session and the level of access that the participant will have during a session.

The presenter may grant remote control permissions. At any point during such a session the presenter can immediately revoke the participant's remote control privileges by pressing Ctrl+F12 (or Ctrl+ESC on a Mac computer) on the keyboard or by clicking on the M icon in the system tray and selecting Disable Remote Control. This allows full control over what can occur during times of remote control.

The organizer may actively request remote control privileges. The presenter always has to explicitly agree to grant remote control rights. It is not possible to control the computer without the explicit consent of the presenter. Both, organizer and presenter can switch the viewing direction. However, the participant first has to explicitly agree to become the presenter and to show their computer screen. After the participant has become the presenter for the first time during a session, the organizer can take back presenting rights for themselves and become the presenter again even without the consent of the participant. However, when switching the viewing direction, the organizer always has to explicitly agree to become presenter. Both, organizer and presenter can end the session at any time.

## Infrastructure Security

Mikogo maintains a distributed network of high-speed switching servers. Session data originating from the presenter's machine and arriving at the participants' machines is switched – never stored – through the Mikogo switching server network. No session data is stored on the Mikogo servers.

There is no need to upload content to the Mikogo servers prior to a session. Dynamic session content displayed during a Mikogo session originates only from the presenter's machine. The participant sees only representations of this data. At the conclusion of a session, all such representations dissipate. All that remains of a Mikogo session is ancillary information like billing records, not a record of the conversation itself.

Snapview invests a lot of time and energy into developing, deploying and maintaining a secure environment for the Mikogo services. We employ state of the art firewalls, network monitoring, and intrusion detection tools. Strict change management is employed and additional internal security policies and procedures are enforced.

## Conclusion

Snapview pays careful attention to the incorporation of security principles and standards in the design and operation of the Mikogo infrastructure and services. The data security of Mikogo will remain the highest priority at Snapview, enabling us to continue achieving the goal of providing efficient and secure online real-time communication services.