

NETOP™

Live GUIDE™

Rich Media Chat for Your Web Site

Product White Paper

System architecture and security

Contents

1	Introduction	1
2	Client side architecture	1
2.1	Netop Live Guide operator console	1
2.2	Netop Live Guide customer console	2
2.3	Netop Live Guide Administration	3
3	Server side architecture	4
4	Security architecture	5
4.1	Protocol overview.....	5
4.1.1	RTMPS.....	5
4.1.2	HTTPS	6
4.1.3	AMF	6
4.1.4	TCP sockets	6
4.2	Secure Sockets Layer (SSL)	6
4.3	Minimum software and hardware requirements.....	7
4.4	Flash Player	8
4.5	Security features	8
5	Sources of information.....	8

1 Introduction

This document focuses on Netop Live Guide system architecture and on system security and is intended for IT managers and system administrators.

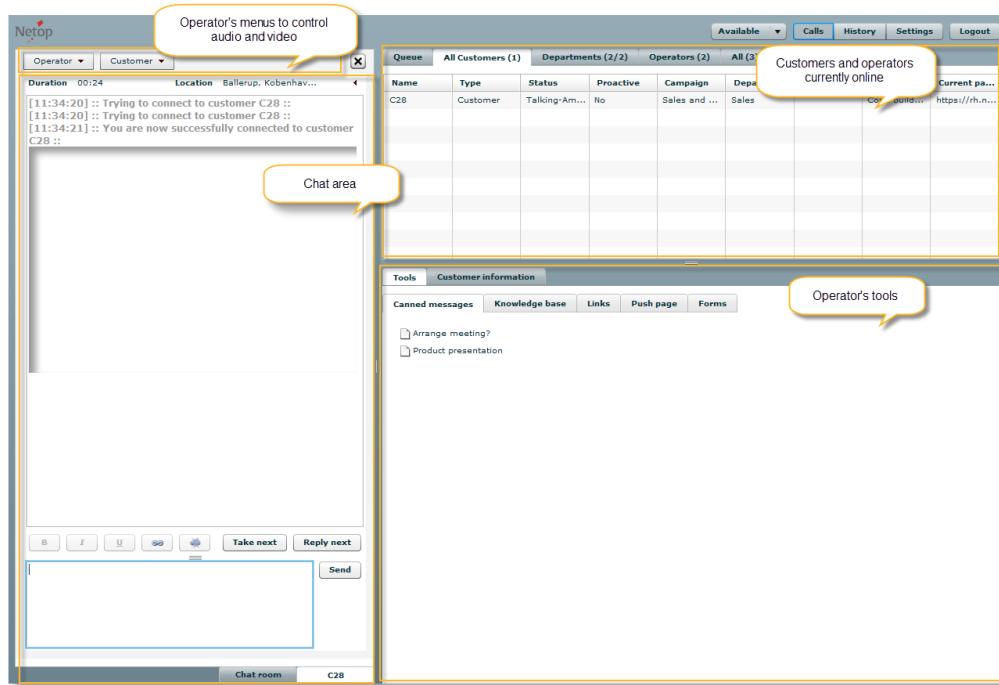
2 Client side architecture

Live Guide client side consists of three components: an operator console, a customer console and an administration module. The components are all accessible through a Web browser, for example Internet Explorer, Firefox, Chrome or Safari.

Adobe Flash Player is required by all three components.

2.1 Netop Live Guide operator console

Netop Live Guide operator console is a Web-based contact center. Incoming calls are placed in a queue and the operators who take calls can use text chat, audio and video.



When an operator has picked up a call, these tools are available:

- See call history from previous calls from the same customer
- See the customer's geolocation
- Transfer call to another operator or department
- Retrieve the URL where the call was made from
- Ban users that behave inappropriately
- Use predefined texts in chat
- Send predefined links to the customer
- Redirect the customer to a specific Web page
- 2-way text chat
- 2-way audio
- 2-way video

All communication is 128-bit SSL encrypted and operators log in with user name and password to access the Web-based contact center. No download or installation is required.

The contact center can be configured so that only operators from specific IP addresses can gain access. Operator access is protected from computer login attempts: after five consecutive failed logins, the operator has to type letters and digits from a distorted image.

The operator console uses SWF Verification. That means that connection will fail for any user trying to connect to the operator console using a different SWF file from the one provided. The verification is handled by the server.

If an operator is temporarily disconnected due to network instability, the connection will automatically be restored if the network connection becomes available again within 15 seconds. This means that short connection interruptions will not impact customers who will not experience any loss of connection.

2.2 Netop Live Guide customer console

Netop Live Guide customer console provides instant messaging features to the customer.



The customer can communicate with an operator in real-time by contacting the operator through a Web page: The customer clicks a button on a Web page and Netop Live Guide opens in a new window.

Live Guide may be set up to automatically offer help to a customer who has been browsing a Web page for a configurable period of time so that the customer can simply click a "yes, I would like assistance" button.

When a customer initiates contact, the customer call is placed in a queue waiting to be answered by an available operator. When an operator answers the call, these tools are available to the customer:

- Choose which department to contact; alternatively the customer is routed to a specific department.
- Access help information on the use of the tools available.
- Get an e-mail transcript of the text chat
- Print the text chat
- Adjust text chat font size
- 2-way text chat
- 2-way audio – unless the operator has disabled this feature
- 2-way video – unless the operator has disabled this feature

All communication is 128-bit SSL encrypted. No download or installation is required.

The customer console uses SWF Verification. That means that connection will fail for any user trying to connect to the operator console using a different SWF file from the one provided. The verification is handled by the server.

The customer console can be reached from any device that has an Internet connection and will automatically scale to fit the actual device.

2.3 Netop Live Guide Administration

Netop Live Guide Administration is a collection of tools for the system administrator to create the customer console, to create tools for the operators and to monitor data collection from customers contacting operators.

These features are available:

- Create and edit departments
- Create and edit operator information
- Create and edit operator tools, including forms to be pushed to customers
- View and delete banned customers
- Create and edit campaigns
- View and search chats and customer data
- View and export reports
- Create customer call button implementation code
- Control which domains the call button can be displayed in.

The above list is an overview only; details available in other Live Guide documentation.

All communication is 128-bit SSL encrypted and system administrators log in with user name and password to access the Administration module. No download or installation is required.

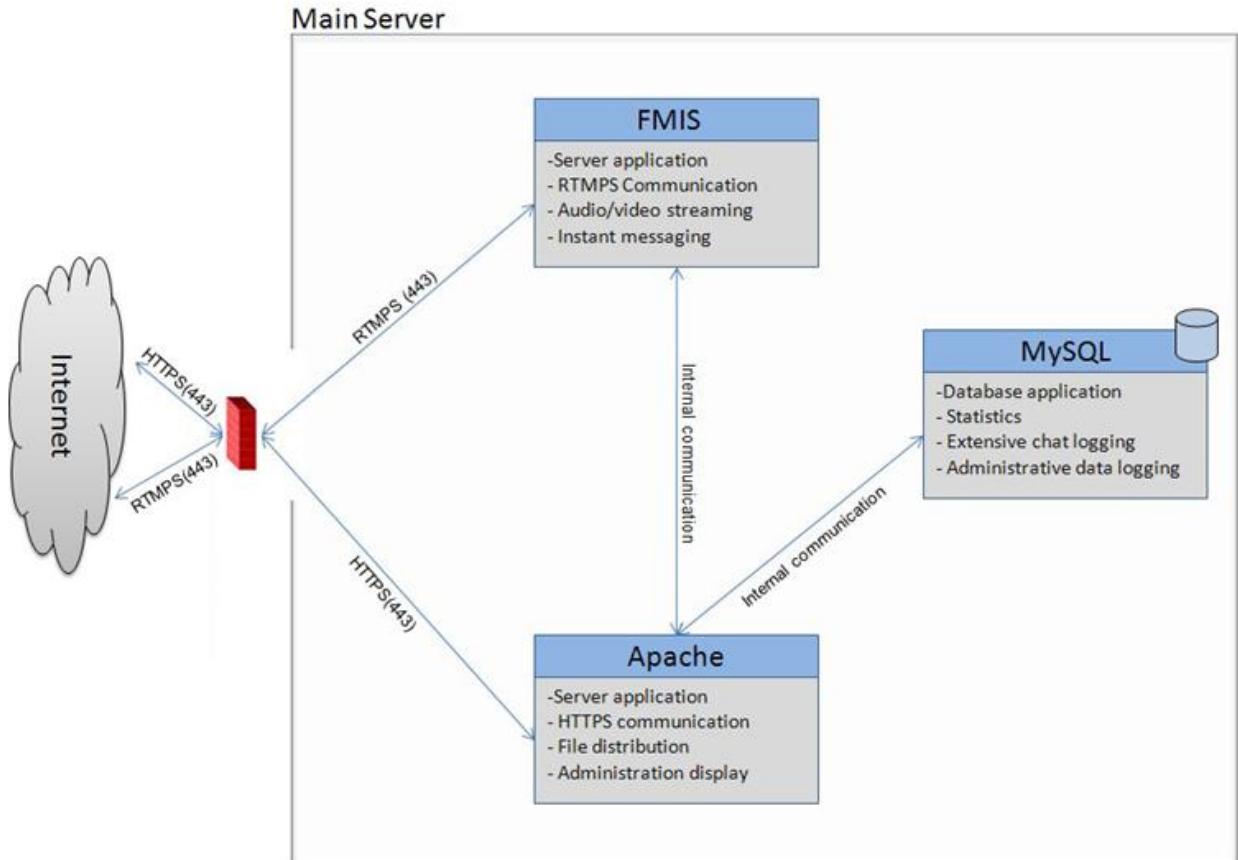
The Administration module can be configured so that only system administrators from specific IP addresses can gain access.

By listing the relevant domain names, the system administrator controls where the customer console interface, the call button, can be displayed.

3 Server side architecture

Live Guide server architecture consists of three components: a web server, a database and a communication server. The Web server is an Apache HTTP Server and the server side programming language used for Live Guide is PHP. The database server is MySQL. The Live Guide communication server is an Adobe Flash Media Interactive Server.

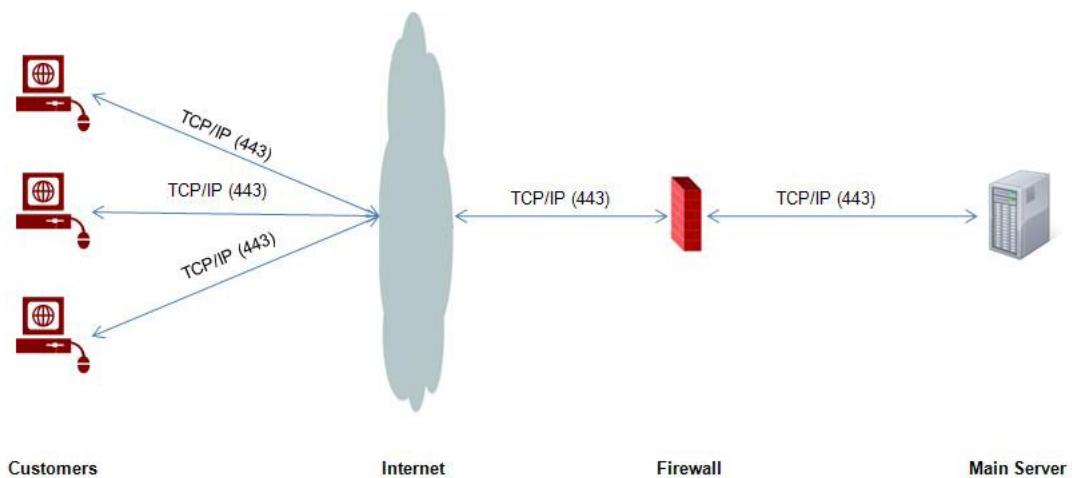
Logical system architecture



4 Security architecture

One of the core focuses of Live Guide is security. Live Guide is primarily a communication tool. This means that one of the main things that need to be taken care of is securing the actual communication between the components. SSL encryption has been used throughout the application. That applies both to the regular Web protocol (HTTPS) and to the communication protocol (RTMPS).

Simplified overview



4.1 Protocol overview

Live Guide uses a wide range of network protocols. The following sections provide a brief overview.

4.1.1 RTMPS

Flash Player uses the Real-Time Messaging Protocol (RTMP) for client-server communication. This is a TCP/IP protocol designed for high-performance transmission of audio, video, and data messages. Although RTMP in and of itself does not offer security features, Flash communications applications can perform secure transactions and secure authentication through an SSL-enabled Web server.

The end result is RTMPS in Live Guide. This protocol is RTMP sent over an SSL. SSL is a protocol that enables secure TCP/IP connections. (Flash Media Server natively supports both incoming and outgoing SSL connections.) The default port is 443. Encryption with Flash Media Server with RTMPS is done in real-

time.

Flash Player cannot access bitmap data or sound spectrum data for media loaded from RTMP sources, although it can display bitmaps and play sounds loaded from these servers.

Flash Player also provides support for versions of RTMP that are tunneled through HTTP and HTTPS. RTMPT refers to RTMP transmitted within an HTTP wrapper, and RTMPS is RTMP transmitted within an HTTPS wrapper.

4.1.2 HTTPS

HTTPS (HTTP over Secure Sockets Layer) is designed to transmit individual messages securely. SSL creates a secure connection between a client and a server, over which any amount of data can be sent securely. SSL works by using a private key to encrypt data that is transferred over the SSL connection. Flash Player uses the operating system or browser to determine whether its data was obtained over a secure HTTPS connection, and records that fact (for instance, by using separate sandboxes). Data loaded from HTTPS sites is subsequently treated differently than data from HTTP or other, less secure, sources.

4.1.3 AMF

Flash Player handles serializing and deserializing ActionScript objects to and from a proprietary terse binary data format called ActionScript Message Format (AMF). AMF serialized objects are the payload of HTTP requests and responses sent between the Flash Player client and the application server. AMF is also used for communication between FMIS and the Web server.

The client-side ActionScript libraries provide the ActionScript objects that a Flash developer uses to connect to and invoke methods on components in the application server. The libraries also provide objects that are helpful for debugging the connection

4.1.4 TCP sockets

Transmission Control Protocol (TCP) is used as the underlying protocol for most of the previously described transmission methods. It does not provide any inherent capabilities for securing the data that it transmits.

4.2 Secure Sockets Layer (SSL)

PKI (Public Key Infrastructure) is built into all Web browsers that use SSL and Flash Player uses the browser to do all the work in the interpretation of client-side PKI and in using the browser's certificate store. An SSL connection is secured by using the PKI certificate of the Web server to share a symmetric key with the Web browser that is used to encrypt data exchanged between them. When SSL is being used to communicate with a Web server, the security functions of the Web browser may allow the end user to view and check the validity of the associated Web server's certificate.

Because Flash Player does not itself implement SSL, all behavior related to certificate verification is determined by the browser. This approach simplifies administration of the client, but it may also result in some variation in behavior between different browsers and operating systems. For example, the symmetric key size and the specific algorithm used for an SSL connection are negotiated by the browser. Similarly, Flash Player does not handle client behavior for certificates that are expired, revoked, self-signed, or do not match the URL of a requested resource.

4.3 Minimum software and hardware requirements

Component	Recommended hardware (minimum)	Recommended software
Operator console	Pentium4 1.6Ghz/1GB ram Mac G4 1.33Ghz/1GB ram	OS: Windows XP SP3/Windows Vista/Windows 7/ Mac OS 10.6 Browser: Firefox 3.5 or later/ Internet Explorer 7.0 or later/ Safari 5.0 or later / Chrome 10.0 or later Adobe Flash Player: Flash Player 10.0.22.87 or later (to achieve maximum security we recommend an upgrade to latest release available)
Customer console	Pentium4 1.6Ghz/1GB ram Mac G4 1.33Ghz/1GB ram	OS: Windows XP SP3/Windows Vista/Windows 7/ Mac OS 10.6 Browser: Firefox 3.5 or later/ Internet Explorer 7.0 or later/ Safari 5.0 or later / Chrome 10.0 or later Adobe Flash Player: Flash Player 10.0.22.87 or later (to achieve maximum security we recommend an upgrade to latest release available)
Administration		OS: Windows XP SP3/Windows Vista/Windows 7/ Mac OS 10.6 Browser: Firefox 3.5 or later/ Internet Explorer 7.0 or later/ Safari 5.0 or later / Chrome 10.0 or later Adobe Flash Player: Flash Player 10.0.22.87 or later (to achieve maximum security we recommend an upgrade to latest release available)

4.4 Flash Player

The Adobe Flash Player on which the Live Guide customer and operator console are built is a highly secure platform that safeguards the data and privacy of the users. The Adobe Flash Player uses the sandbox security model which further ensures that user data and local file system is not accessible. Additionally all data is SSL (Secure Sockets Layer) encrypted with a 128-bit encryption.

4.5 Security features

The solution offers other security features such as

- Brute Force protection on the administration and operator console.
- Control of which domains that are allowed to use the call button.
- IP restrictions on the administration and operator console.
- Encoded IDs in the URLs.
- SWF verification for protection against reverse engineering of the Flash files.

5 Sources of information

Description	Source
Adobe Flash Player Security	http://www.adobe.com/products/flashplayer/security/
MySQL® Technical White Paper	http://www.mysql.com/why-mysql/white-papers/integrity.php
Flash Media Server White Paper	http://www.adobe.com/products/flashmediaserver/pdfs/fms3_5_wp_ue.pdf
Apache documentation	http://httpd.apache.org/docs/

About Netop

Netop develops and sells market leading software solutions that enable swift, secure and seamless transfer of video, screens, sounds and data between two or more computers. The company has three business areas: Administration, Education and Communication.

In Administration, Netop Remote Control is the most secure, trusted and scalable remote support solution on the market today. Used by more than half of the Fortune 100, it helps businesses reduce support costs and meet security and compliance standards. In Education, Netop is the world leader in classroom management software, helping teachers in 75 countries make teaching with technology easier and more effective. Higher efficiency and better grades are some of the results. And in Communication, Netop Live Guide is the live chat solution that helps companies provide better customer service, increase efficiency and sales, and turn website visitors into customers.

Headquartered in Denmark, Netop employs 130 people and has subsidiaries in the United States, Great Britain, China, Romania and Switzerland. The company sells its solutions to public and private clients in more than 80 countries. Netop Solutions A/S shares are listed on the Copenhagen Stock Exchange OMX. Read more at: www.netop.com.