TECHNICAL ARTICLE

NETOP®

Live GUIDE™

Live Chat for Customer Engagement

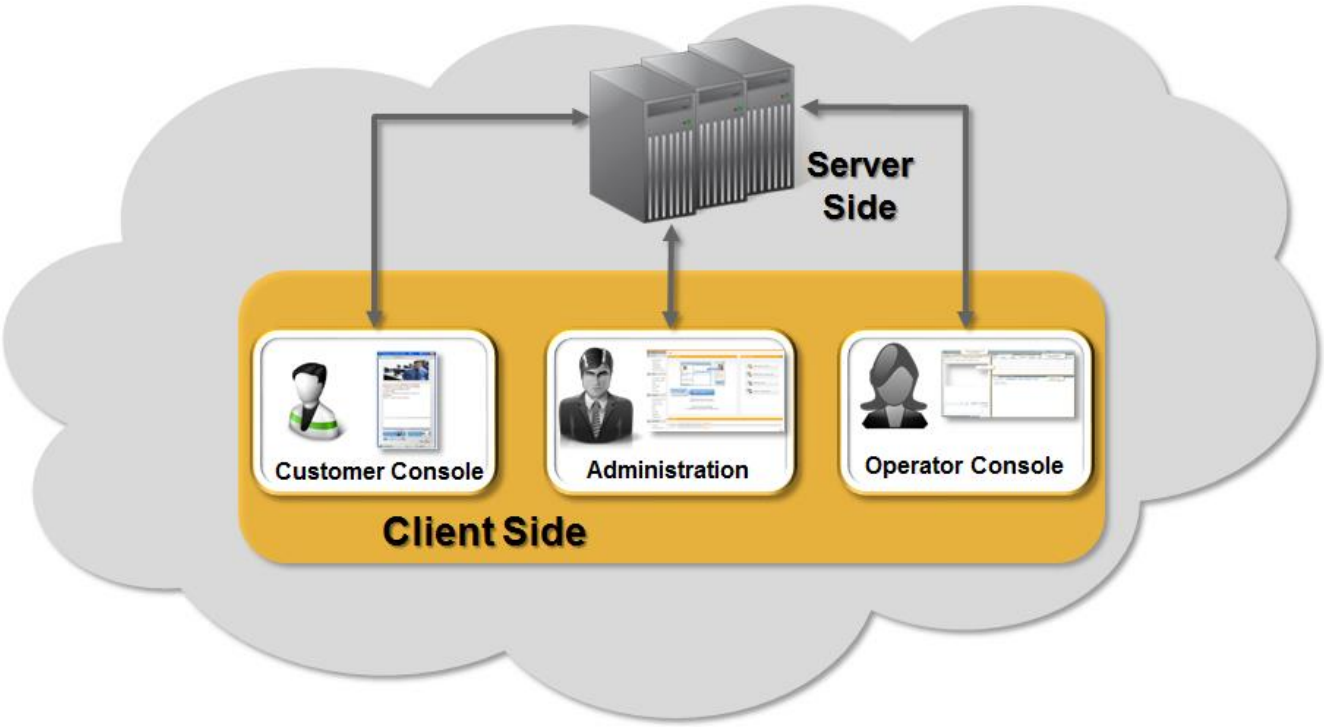
Live Guide – System Architecture and Security

Contents

1. Introduction

Netop Live Guide is a cloud-based live chat browser based system.

You can see below an overview of the Live Guide components.



Note: The Flash plugin is required to run the Operator Console. The Customer Console runs both as Flash and HTML 5, depending on the Customer having the Flash plugin,

Live Guide communication is 128/256 bit SSL encrypted based on browser's configuration.

2. Hosting Environment

Live Guide is hosted on the Amazon Cloud. Some of the security capabilities included (not limited to these) are:

- Recognized attestations, reports and certifications
- Complete audits and risk assessment for customer data
- Control access to own cloud resources at a granular level
- Multi-factor authentication when accessing cloud resources

2.1. Standards - Compliancy

The Live Guide hosting is compliant as seen below:

IT Security Standards	Industry Specific Standards
SOC 1/SSAE 16/ISAE 3402 (formerly SAS70)	HIPAA
SOC 2	Cloud Security Alliance (CSA)
SOC 3	Motion American Association of America (MPAA)
PCI DSS Level 1	
ISO 27001	
ITAR	
FIPS 140-2	
FedRAMP(SM)	
DIACAP and FISMA	

To read more information about these security standards, see http://aws.amazon.com/compliance/.

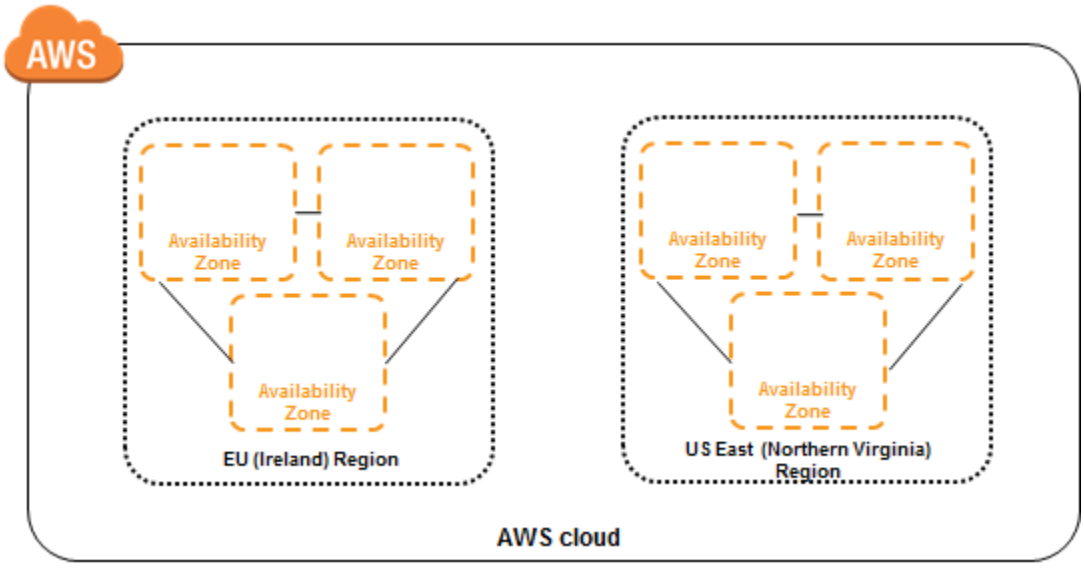
2.2. Business Continuity Management

Amazon's load balancing infrastructure has a high level of availability allowing us to deploy a resilient IT architecture.

2.2.1. Availability

We took advantage of AWS infrastructure including multiple data centers, which are redundantly connected to multiple tier-1 transit providers, and in order to remain resilient in front of failures, we have distributed the Live Guide servers across multiple availability zones in the following regions:

- EU (Ireland) Region – serving the EU customers
- US East (Northern Virginia) Region – serving the US customers



Each region is completely independent, achieving the greatest possible fault tolerance and stability Each Availability Zone is isolated, but the Availability Zones in a region are connected through low-latency links.

2.2.2. Incident Response

Netop Operations team provide 24x7x365 coverage to detect incidents and to manage the impact and resolution. For more information on Netop product maintenance and support services, see Netop Service Level Agreement.

2.3. Network Security

Secure Network Architecture Network devices, including firewall and other boundary devices, monitor and control communications at the external boundary of the network and at key internal boundaries within the network.

2.3.1. Transmission Protection

Connection to an AWS access point is done via HTTPS. For additional layers of network security, AWS offers the Amazon Virtual Private Cloud (VPC), which provides a private subnet within the AWS cloud.

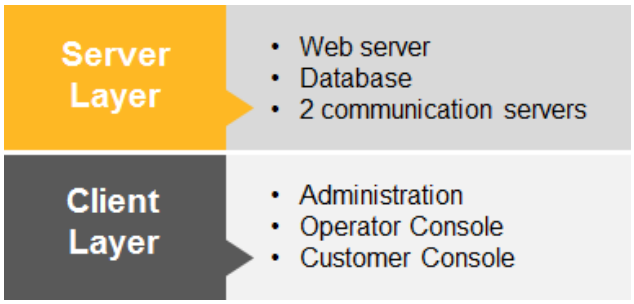
2.3.2. Network Monitoring and Protection

AWS uses a variety of automated monitoring systems to provide high performance services and availability. The tools monitor server and network usage, scan port activities, application usage and unauthorized intrusion attempts. They also allow setting up performance thresholds for unusual activity. Moreover, alarms inform AWS operations and management personnel when warning thresholds are crossed on key operational metrics.

The AWS network provides protection against traditional network security issues: Distributed Denial of Service (DDoS), Man in the Middle (MITM) Attacks, IP Spoofing, port scanning, packet sniffing by other tenants and many more.

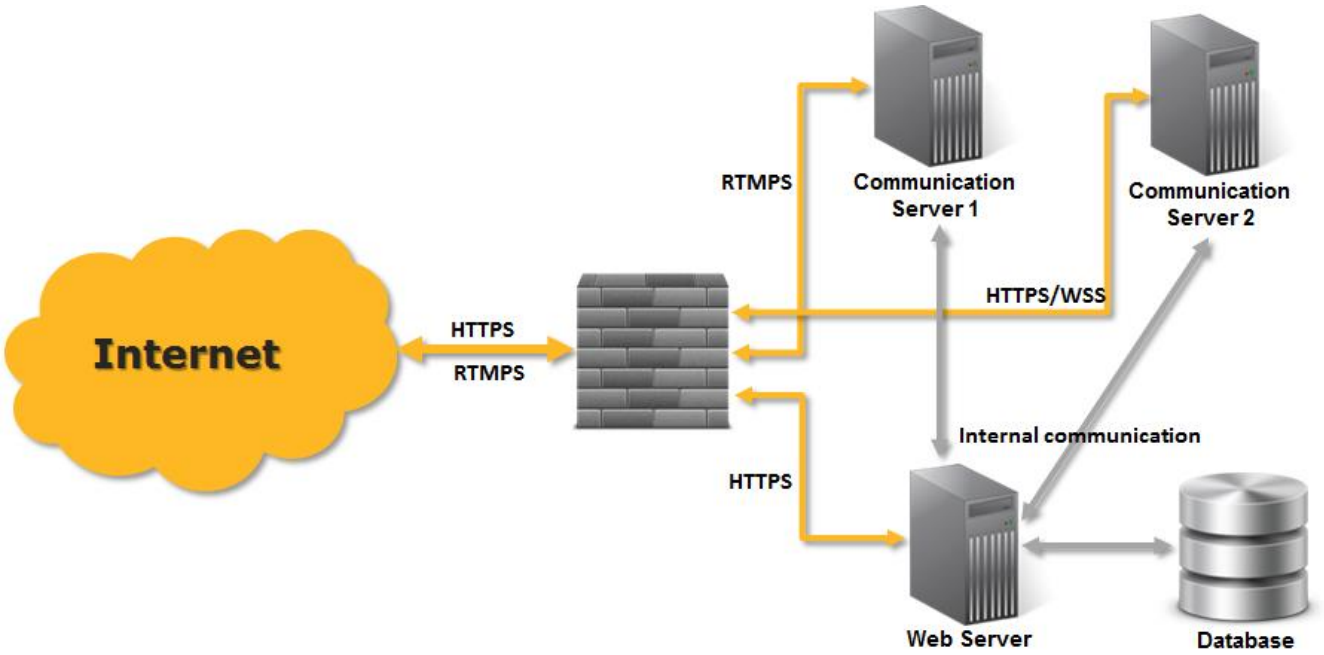
3. Netop Live Guide System Architecture

Netop Live Guide was designed and implemented on two layers: client and server.



3.1. Server Layer Architecture

The server layer uses a Three-Tier architecture model:



3.1.1. Web Server

The presentation tier gives the user access to the application through HTTPS communication. It is responsible for file distribution and administration display.

3.1.2. Communication Server 1

The business logic tier responsible tor RTNP over TLS communication: audio/video streaming and instant messaging for the Customer Console and the Operator Console. Live Guide may also encapsulate RTMP traffic in HTTPS.

3.1.3. Communication Server 2

The business logic tier responsible tor WebSocket / HTTPS communication: Instant messaging for non-Flash customer console.

3.1.4. Database

This is the actual Data tier. The data tier stores statistics, user generated data, administration & configuration information.

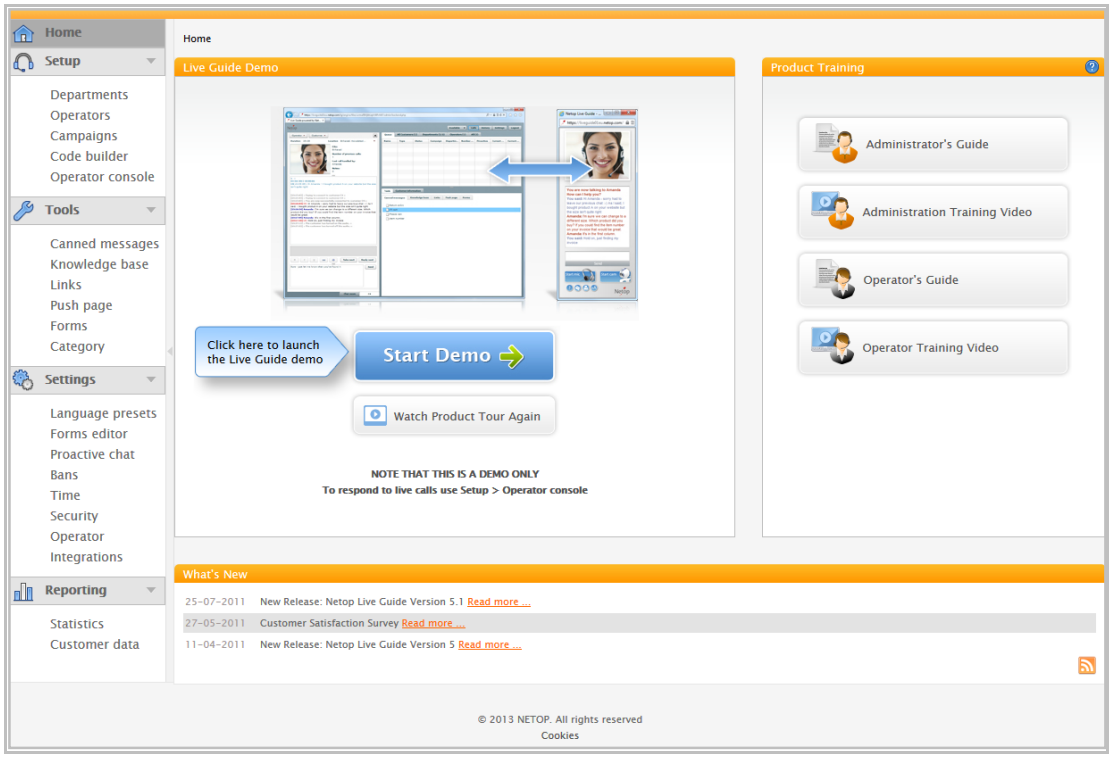
3.2. Client Layer Architecture

Live Guide client layer consists of the following components: Administration, Operator Console and Customer Console.

3.2.1. Netop Live Guide Administration

Netop Live Guide Administration is a collection of tools which target the system administrators who have full access to all features so that they can set up the system. In the implementation phase, system administrators have to perform the following operations:

- Create departments, ensure that operators are created as users, create tools for operators and generate the code for the Web site chat button or the hyperlink to open chat.
- Ensure that the code for the Web site chat button is implemented on the Web site.
- Send logon information to the operators who are going to answer customer chats.



When a chat button has been operational for a period of time, system administrators can review logs of all chats and produce extensive statistics to verify and document system performance and campaign effectiveness.

Security configurations available from the Administration:

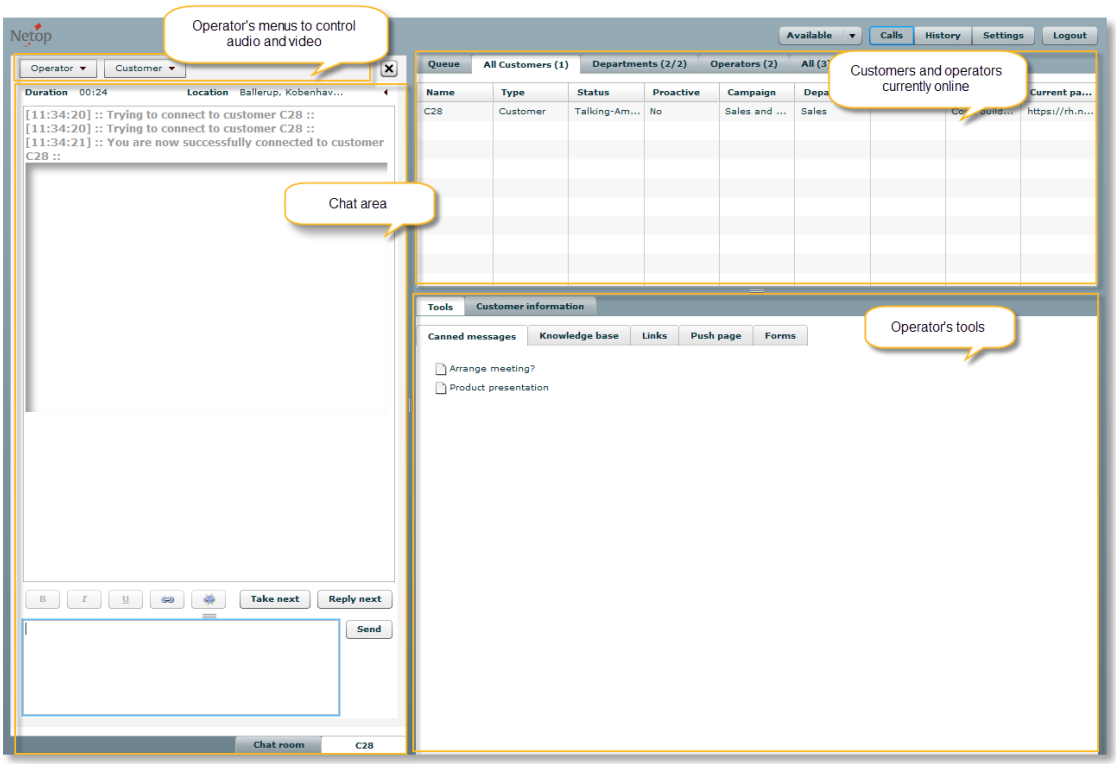
1. The Administration module can be configured so that only system administrators from specific IP addresses can gain access.
2. By listing the relevant domain names, the system administrator controls where in the customer console interface, the call button can be displayed.
3. There is API access available. The access is conditioned by an access token that is generated from the Administration. If for some reason the access token is compromised, it can be regenerated, making the previous one not valid.
4. Audio and Video encryption can be configured from here. Possible options are: None, Low or High.
5. Data storage controlled through the retention period. More information here.

3.2.2. Netop Live Guide Operator Console

The Netop Live Guide Operator Console is browser based area where the Operators get into contact with the Customers (visitors).

Each customer contact session is logged, for example with information about chat duration, campaign and department, to enable you to subsequently do statistics based on the historical data.

The information displayed in the customer calls list can be customized as can the use of colors and the use of audio for various types of alerts.



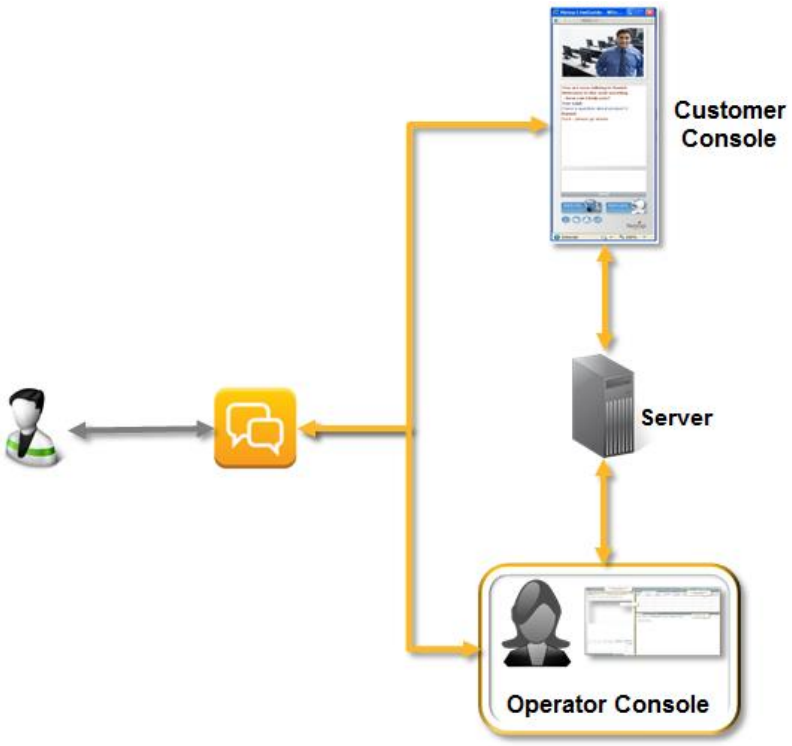
Main features:

- ✓ Online Customer Intelligence: customer's geolocation, capturing customer data for later reference and displaying customer information in real-time
- ✓ Preview chats and forms
- ✓ Advanced routing and workflow
- ✓ Prepared responses and predefined links
- ✓ Audio and video chat
- ✓ Co-Browsing
- ✓ Indication that the customer is typing a message
- ✓ Comprehensive reporting
- ✓ Remote view and assistance
- ✓ Stored history and logs
- ✓ Spell checking
- ✓ Possibility of banning inappropriate customers

3.2.3. 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 or chat text link 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.

The Customer Console can also be launched on smartphones and tablets or on computers that do not have the Flash player plugin installed and HTML 5 is available

3.2.4. Customer Console: Flash versus HTML5

Feature	Flash	HTML 5
Choose which department to contact; alternatively, the customer is routed to a specific department	Yes	Yes
Help	Yes	Yes*
Domains	Yes	Yes
Real-Time API	Yes	Yes
Get an e-mail transcript of the text chat or print the text chat	Yes	Yes*
Adjust text chat font size	Yes	Yes*
Text chat	Yes	Yes
Print chat text	Yes	Yes*
2-way audio and 2-way video – unless the operator has disabled these features	Yes	Yes
Forms	Yes	Yes
Co-Browsing	Yes	Yes
Indicator that the operator is typing a message	Yes	Yes

* These features are available from the **Settings**  icon.

4. Netop Live Guide Security

The Netop team is aware that delivering secure products is the key to operate in the best interest of the clients, securing data and communication.

4.1. Application Security

Live Guide communication is never Peer-to-Peer (Customer-Operator) over the internet, but through secure, off-site servers.

4.1.1. Communication Security

Live Guide is safely secured via Secure Socket Layer (SSL). SSL encryption applies to both the regular Web Protocol (HTTPS) and to the communication protocols (RTMPS and WSS).

Real-Time Messaging Protocol Secure (RTMPS)

By default, Live Guide utilizes RTMP over TLS to the liveguidefms01eu.netop.com server and may fall back to using RTMP over HTTPS, depending on the network proxy configuration. Live Guide will always use RTMP over HTTPS if configured as such (under **Settings** > **Security** > **Connections)** .Depending on configurable security settings (under **Settings** > **Security>Connections**) Live Guide may also use plain RTMP for audio and video.

Your firewall or other hardware/software defense should be configured to allow two-way communications to Live Guide servers on port 443. If you have audio and video configured to run with encryption set to **None**, you need to have port 1935 open as well.

No other ports are required by the Live Guide services.

SWF verification

The Operator console and Customer console flash files are fully protected against reverse engineering or modifications and only if the file is successfully verified will the chat session begin.

HTTP over Secure Sockets Layer (HTTPS)

For backward compatibility with restrictive proxies, Live Guide may also encapsulate RTMP traffic in HTTPS depending on configurable security settings in Live Guide Administration under **Settings** > **Security** > **Connections.**.

WebSocket Secure (WSS)

WebSocket is an independent TCP-based protocol providing full-duplex communications channels over a single TCP connection. WSS is WebSocket transported over TLS.

Live Guide offers a secure two-way live communication via WSS.

ActionScript Message Format (AMF)

AMF is a compact binary format that is used to serialize ActionScript objects and XML. In Live Guide, AMF is used in conjunction with RTMPS to establish connections between the Communication Server 1 and the Web Server and to control commands for the delivery of streaming media.

4.1.2. Authorization and Authentication

Live Guide customers designate the administrators who have the authority to access and manage login accounts.

We have a set of password rules for the Operator's Console:

- The password must be at least 8 characters long.
- The password must include at least one upper case letter and one digit.
- The password must include at least one special character

4.1.3. Live Guide Access Restrictions

Live Guide enables you to set up tight control of which IPs are allowed to access both the Operator Console and Administration module; this is done by allowing access from specific IP addresses only. When IP access has been defined even users who have the correct user name and password are denied access if they are not accessing from a computer on the IP access list.

4.1.4. Data Storage

Live Guide stores customer generated data on its servers for a maximum period of 18 months. This is called the Retention Period. It always refers to the most recent data. Your Live Guide administrators may choose to set a different Retention Period.

4.1.5. Security Audits and Reporting

Netop Operations periodically performs external scans on the production system and periodic audits on the Live Guide data in order to identify potential security issues.

Netop Operations are able to identify security events and critical information and furthermore analyse and establish action points to ensuring system availability, performance and security.

5. Technical Requirements

Overall recommended hardware

- Pentium 4 1.6Ghz/1GB RAM
- Mac G4 1.33Ghz/1GB RAM

Recommended software

- **OS**: Windows XP SP3 / Windows Vista / Windows 7 / Windows 8 / Windows 8.1 / Mac OS 10.5 / MAC OS 10.6 / MAC OS 10.7 / MAC OS 10.8 / MAC 10.9
- **Browser**: Internet Explorer 7.0 or later / Firefox latest version / Safari latest version / Chrome latest version
- **Adobe Flash Player**: Flash Player latest version (a minimum requirement would be Flash Player 10.0.22.87 or later).
- **Mobile**: iOS 5.1.1 or later, default browser; Android 4.1.1 or later, default browser.

6. Resources

- Amazon Security Whitepaper – http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf
- Amazon Regions and Availability zones – http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html
- Adobe® Flash® Access™ Overview on Protected Streaming – http://www.richinternet.de/attachments/084_flashaccess_wp_protectstreaming.pdf
- Amazon Web Services Whitepapers - http://aws.amazon.com/whitepapers/
- About WebSockets - http://en.wikipedia.org/wiki/WebSocket, http://msdn.microsoft.com/en-us/library/windows/apps/hh761446.aspx, http://blog.kaazing.com/2012/02/28/html5-websocket-security-is-strong/