System and Deployment Guide

XLeap In-house Server

Contents

Documentation

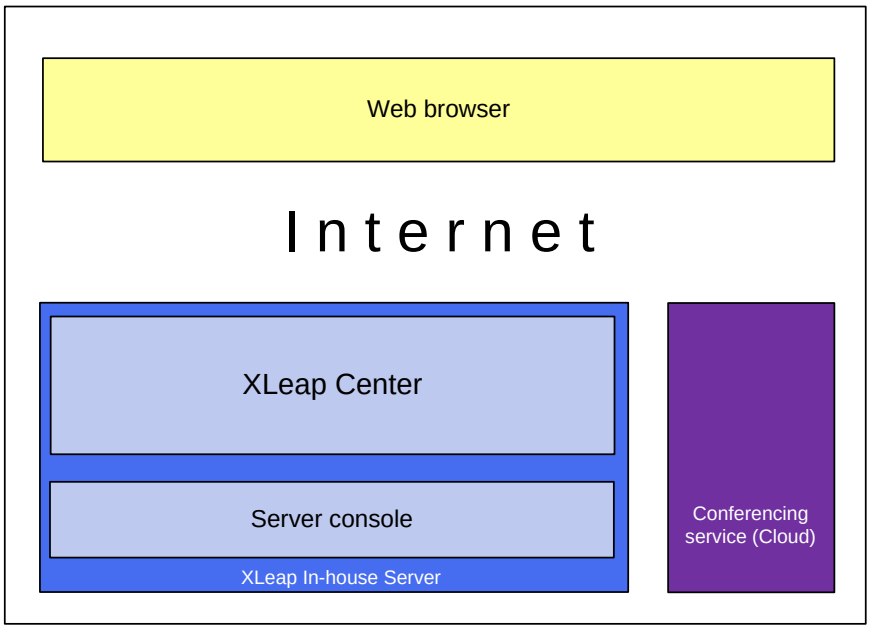
This Deployment Planning Guide is the starting point for deployment of an XLeap In-house Server.

Installation of the XLeap In-house Server is described step-by-step in a separate Installation Guide. Specific administrative concepts, functionalities and tasks are covered in the Server Administration Guide and the Center Administration Guide.

If you are concerned with the SCIF Edition of the XLeap Server which is designed for deployment on highly secured Intranets from which there can be no "reporting back" to the XLeap licensing system, check out the specific Systems and Deployment Guide for the SCIF Edition.

Download the latest documentation from XLeap's website.

1. System requirements



Components of the XLeap solution

An XLeap In-house Server is an installable enterprise-class web application server which provides a group decision support system (GDSS) with a set of interactive workspaces for use in decision making sessions and workshops. Sessions are run from the XLeap Center which holds all user data and session content. Deployment on the network is controlled by the Server console. Conferencing relies on the cloud-based conferencing service which is merely a conduit for real-time

communication (video, voice, screen sharing) between clients. The conferencing service does not hold personally identifiable customer information or content.

The XLeap Center is a web application based on HTML5 (Angular2+).

1.1 The XLeap (browser) client

XLeap runs on all popular devices.

Users can switch the GUI language between English (default) and German.

1.1.1 Client software requirements

XLeap runs in recent versions of all popular browsers. XLeap does not require downloads, plug-ins, or add-ons.

- **Chrome** from version 81 (Recommended)
  Chrome is fully compatible also on Chromebooks and Mac. Older versions (from v76) can join XLeap sessions without a conference.*
- **Edge** from version 79
  Edge (Chromium) is fully compatible. Legacy versions (from v16) can join XLeap sessions without a conference.*
- **Firefox** from version 76
  Firefox is fully compatible.
- **Opera** from version 68
  Opera is fully compatible.
- **Safari** from version 13
  Safari is fully compatible. Older versions (11, 12) can join XLeap sessions without a conference.*

Limited compatibility:

- **Internet Explorer 11**
  Internet Explorer 11 does not support XLeap conferencing. It can join XLeap sessions without a conference.*

Tablets and phones

By their design, mobile devices only support passive screen sharing.

Android. Users of Android 7+ tablets or smartphones use Chrome or Firefox.

iOS. Users of iPads or iPhones use Safari from version 13. Older versions (11, 12) can join XLeap sessions without a conference.

** XLeap sessions which run over an extended period of time ('anytime sessions') typically do not require the conferencing service and will admit participants with legacy browsers that would not*

meet the requirements of the conferencing service. This is also true for sessions which use a 3rd-party conferencing service.

1.1.2 Client network requirements

Users require access to the

- XLeap Center via port TCP 443 (HTTPS). XLeap automatically redirects incoming HTTP connections to a secure SSL (TLS) connection.
- XLeap conferencing services (WebRTC; session.voxeet.com) via
  - UDP 20,000 - 65,000
  - fallback TCP 443

XLeap connections are robust. Should a connection be broken, users simply log in again. Only content that has not been posted will be lost.

Use of an SSO service requires that relevant users can also access that service.

1.2 The XLeap In-house Server

XLeap In-house Server runs on 64-bit ("x86_64") Intel (compatible) processors.

1.2.1 Server software requirements

XLeap In-house Server runs on popular Linux distributions and Windows Server. The server deploys its own embedded databases. In a 2-tier deployment, customers can choose between MS SQL Server or MySQL-compatible database servers for the XLeap Center database.

Table 1: Software requirements XLeap In-house Server

Supported operating systems	Supported databases
(64-bit versions required)	Apache Derby (embedded)
Amazon Linux 2	MS SQL Server 2016 or later
CentOS Linux 7 or later	MySQL 5 (compatible) or later, e.g. Aurora
RedHat Enterprise Linux 7 or later	
Windows Server 2016 or later	

A cryptographically unique installer is created for each installation and provided for download. Execution of the installer requires “root” privileges (Windows: “Administrator”). On Linux, the server process runs with limited privileges.

The installer checks the installation prerequisites*, and installs

- an OpenJDK 8 Development Kit
- the Server console application

- the XLeap Center application (embedded Tomcat 9)
- the embedded database (Apache Derby).

** Windows Servers must run Java (any contemporary JRE) to execute the installer which is delivered as a '.jar' file.*

XLeap strongly recommends installation of the server on a (virtual) instance that is dedicated to this purpose.

Databases other than the embedded database are typically deployed on a separate instance dedicated to that task.

1.2.2 Server resource recommendations

Performance of the XLeap In-house Server depends on effective caching of database information and immediate "write-through" access to the database. For this, the server should be optimized for RAM size and disk speed:

- Processor: Any contemporary server CPU will take you a long way. Faster is better.
- RAM: From 8 GB. 16 GB recommended for larger deployments; more is better
- 500GB SSD or a fast network storage

  Allocation of space depends primarily on the number and size of file attachments – not sessions

In a 2-tier setup, the connection to the database server must be fast.

XLeap Server runs in virtualized environments.

Disclaimer. While the subscription agreement for XLeap Servers does not restrict the number of Hosts, concurrent sessions, and participants, no system can technically meet such a contractual possibility. To date, XLeap is unaware of any limitations in scalability of the server that cannot be overcome by configurations and hardware currently in use in contemporary data centers. This said, actual resource requirements depend on actual use patterns and will differ considerably between organizations who make heavy use of, say, file attachments or of exporting (encrypting) & importing (decrypting) sessions and templates and those who simply run many sessions. Further, the impact on resource requirements of future functionality or of changes to the (network and client) environments cannot be predicted.

A case in point is the cloud-based conferencing service. Conditions on the Internet permitting, this service will support anything that can reasonably be called a meeting or workshop. It is not designed for mass communication.

XLeap will work with its customers to overcome barriers to scalability should they occur.

---

2. Deployment

The requirements and options for deploying a XLeap In-house Server are given below. The description assumes an Internet deployment. It points out possible restrictions and their practical implications.

2.1 Basics

XLeap Servers run 2 applications: First, the administrative Server console (see chapter Server console) and, second, the XLeap Center on which XLeap sessions are created, run and stored.

This deployment guide is primarily concerned with the prerequisites for execution of the installer, the configuration of the server on the in-house (data center) network and its accessibility from the Internet. Further, it discusses administrative restrictions at server level, by which the options of Center administration can be limited.

These fundamental settings are made by the initial Server administrator 'serveradmin' in the Server Console. 'serveradmin' can assign up to 3 individuals as Server administrators. If so, these 'real person' administrators would then usually lock the default 'serveradmin' account.

2.2 Privileges of the XLeap process

On Windows servers, the XLeap process* runs with "System" privileges.

On Linux servers, the XLeap process runs with limited privileges (user 'meetingsphere'*). SELinux must be disabled or 'permissive'.

** Previous versions of XLeap were branded 'MeetingSphere'. Legacy designation 'meetingsphere' is maintained for the XLeap process and installation directory for backward compatibility.*

2.3 Database

XLeap Servers deploy two databases:

The Server console uses a dedicated instance of the embedded database (Apache Derby).

The XLeap Center application also uses an embedded instance of Apache Derby. After installation of the server, this database can be migrated to a 2nd-tier database server. This is recommended for large deployments (many users, many sessions).

Migration. The XLeap Center database may be migrated between supported databases. Migration requires temporary shutdown of the XLeap Center and specification of the target database server. The time required for the migration depends on the volume of data to be migrated and the performance of the systems involved.

Backup. For backup, XLeap Servers rely on the regular backup mechanisms of the data center such as periodic (incremental) snap-shooting of the server's file system.

2.4 Incoming connections

There are three mandatory types of incoming connections to an XLeap In-house Server:

1. Server administrators connecting to the Server console,
2. Hosts, participants, and administrators connecting to the XLeap Center,
3. XLeap's licensing system connecting to the XLeap Center.

Use of an SSO identity service (SAML2.0) requires connections to and from that service.

If your Information Security Policy does not allow for a connection to/from the XLeap licensing system, you may want to opt for the SCIF Edition of the XLeap Server which does not require such connection.

2.4.1 Client connections to the Server console

Server administrators call the Server console with their browsers under the XLeap Center's URL via port TCP 62701 (default), e.g. xleap.example.com:62701. The server will respond to HTTP requests only until the server's TLS certificate has been installed and HTTPS encryption kicks in.

Access to the Server console is usually restricted to the data center's network.

2.4.2 Client connections to the XLeap center

Operation of the XLeap Center application requires installation of a TLS certificate.

Browsers of Hosts, participants and administrators connect to the XLeap Center via TCP 443 HTTPS. Connection attempts via TCP 80 (HTTP) are redirected to TCP 443 (HTTPS).

2.4.3 Incoming connection from the XLeap licensing system

The XLeap licensing system must be able to resolve the (sub) domain name of the XLeap Center and connect to it via TCP 443 (HTTPS) to, e.g.

- deliver new Host subscriptions
- increase or reduce the number of licenses covered by Host subscriptions
- renew or terminate subscriptions

at the customer's order.

Authentication between the XLeap Center and the licensing system occurs by complex bidirectional, dynamic *handshake*-authentication.

2.4.4 Incoming connection from an SSO identity service (optional)

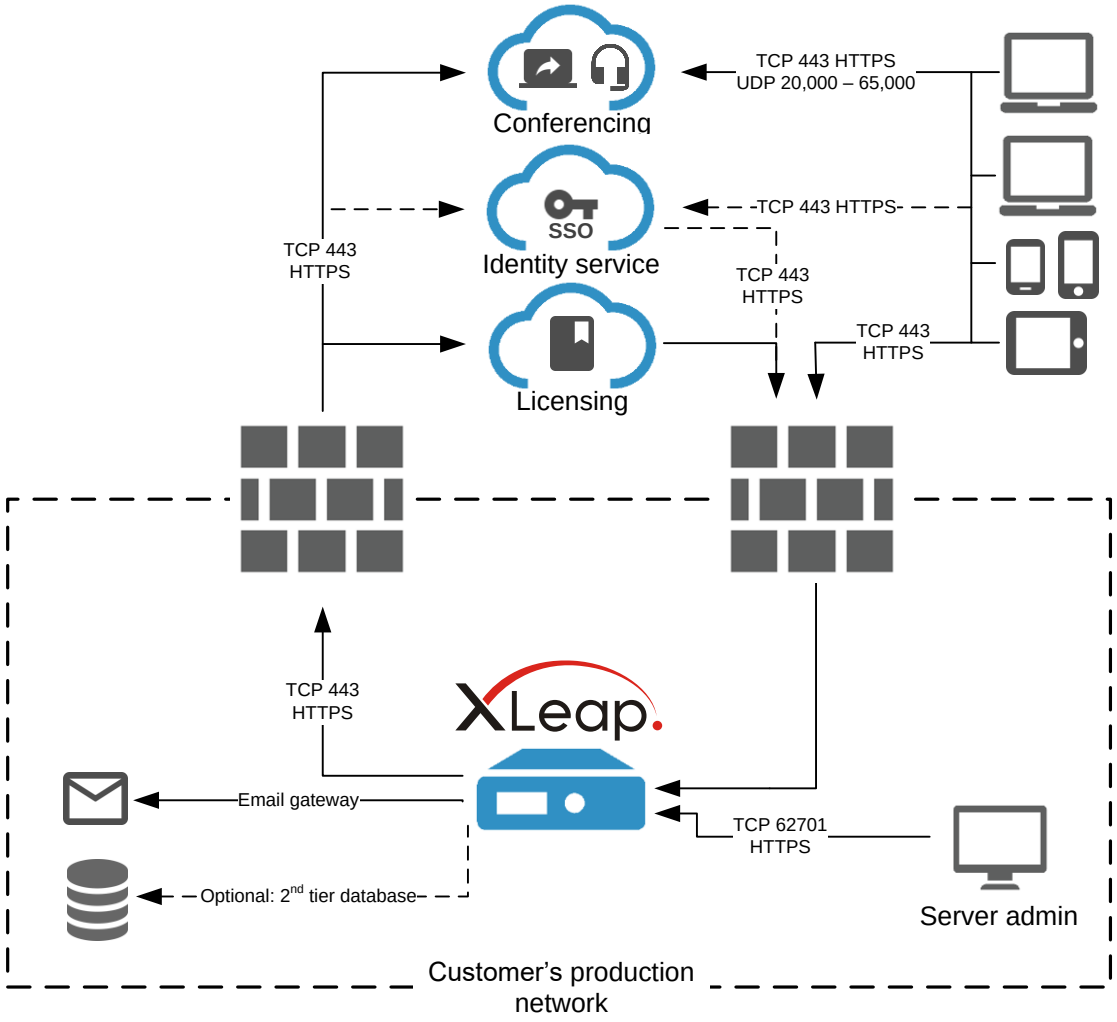
If authentication of some or all users shall occur by an identity service, that service must occasionally check (read) the XLeap Server's SAML metadata via TCP 443 (HTTPS) and, if so, update its records regarding the XLeap Server.

2.4.5 TLS encryption

For incoming connections, the server negotiates TLS 1.3 encryption. For this, it requires a certified keystore which covers the sub domain of the XLeap Center.

2.5 Outgoing connections

The number and nature of outgoing connections depends largely on the deployment scenario i.e. which services the server leverages and where these services sit on the network.



Example: Deployment with SSO

2.5.1 Connection to the XLeap licensing system (required)

XLeap In-house Servers report certain licensing events as listed in section 4 ‘Administration of subscriptions) to the XLeap licensing system, https://store.xleap.net.

An HTTPS-proxy can be specified for this connection.

2.5.2 Connection to email gateway (required)

For sending passwords and user notifications, the XLeap Server requires an outgoing SMTP connection to and a user account on an SMTP (MTA) service.

SMTP, STARTTLS and SMTPs are supported. Ports can be configured at will.

XLeap Servers support use of a SOCKS proxy for SMTP.

XLeap In-house Servers do not *receive* external messages (from other client systems) and have no interfaces with, for example, scheduling or calendaring applications.

The outgoing mail server is configured in the Server console.

2.5.3 Connection to the conferencing service (recommended)

Unless conferencing services i.e.

- Voice and video conferencing
- Screen sharing

are disabled administratively, the XLeap Center must be able to connect to https://session.voxeet.com via TCP 443, if so, via an HTTPS proxy.

Conferencing services coordinate the streaming of voice, video, and screen sharing data between clients. Content touches the service only in transit. It is not recorded or stored.

The XLeap Server controls the creation and closing of conferencing sessions. Coordination with the conferencing service is achieved by unique numerical identifiers representing the relevant conference and client session. The link between these identifiers and XLeap sessions and personally identifiable information such as the names or usernames of participants is maintained exclusively on the XLeap Server. All client access to the conference requires authentication by unique personal access codes which are communicated just in time.

2.5.4 Connection to a database server (optional)

A connection to a customer-supplied database server is only required when such a service is deployed. Ports and protocols depend on the database server.

2.5.5 Connection to an SSO identity service (optional)

If authentication of some or all users shall occur by an identity service, the XLeap Server must occasionally check (read) that service's SAML metadata via TCP 443 (HTTPS) and, if so, update its records regarding the identity service.

3. Single Sign On

XLeap In-house Servers support Single Sign On (SSO) via a SAML2.0 identity service.

The XLeap Server is configured for SSO on the command line and by upload of a .json file which specifies, amongst other things, the email domains of users who shall be authenticated by SSO.

Users whose username falls under SSO

- are defined as 'internal' users
- can be created manually in XLeap
- are maintained by the identity service from first login through that service

Unless administratively disabled, 'external' users will continue to be maintained by user administration of and authenticate against the XLeap Center. For details on administrative concepts under SSO, please check out the Center Administration Guide for the XLeap In-house Server.

Setup of SSO is not trivial and usually involves significant testing between staged instances of the XLeap Server and the identity service.

If you consider use of SSO, tell your XLeap sales representative. XLeap can help by guiding your administrators through the configuration process and even stage an XLeap Server for integration testing on your behalf. Again, talk to your rep about your plans and what support you might want.

---

4. Server console

The console is a separate web application which governs

- Fundamental settings of the XLeap Center such as its database (embedded or customer-installed database server)
- Use of cloud-based conferencing services
- Restrictions on attachment file-size
- Starting or stopping the XLeap Center application
- IP address(es) and ports
- Server administrators
- TLS encryption
- Email (SMTP) gateway

- Log control
- Proxies

The Server console affords its own embedded database (Apache Derby) which is separately backed up whenever a change occurs to the server's settings.

Access is restricted to Server administrators who connect to the console with their browsers via port TCP 62701 (HTTPS, default).

5. Administration of subscriptions

There are two types of subscription:

1. The software subscription for the XLeap In-house Server
2. Host subscription(s) for the required number of Host licenses

Subscriptions are administered i.e. bought, renewed, or terminated by Purchase Order. Changes are implemented online on the XLeap In-house Server.

The licensing of individuals as 'Host' occurs in the XLeap Center's user table by the customer's Subscription administrators and Licensors, see below.

The integrity of XLeap subscriptions is protected by a set of reportable events:

- Appointment of an individual as Subscription administrator or Licensor
- Licensing or un-licensing of an individual as Host
- Changes to a personally licensed user's name or email address
- Changes to the XLeap Server instance's MAC address or system time
- Elapsed time since last connection to the licensing system
- Restore of the Console database

If such an event occurs within the XLeap Center or the Server console, administrators, before saving that change, are warned that they are about to cause an event that is reported to the XLeap licensing system.

6. Administrative roles

A XLeap In-house Server is administered through a set of administrative roles.

6.1 Server administrator

Up to three "Server administrator" accounts can be maintained in the Server console. Beyond administering the settings of the server, Server administrators

- Configure the server's network settings
- Configure the XLeap Center
- Provide temporary administrative 'emergency' access to the XLeap Center
- Shut down and start the XLeap Center

- Check for, download, and apply update installers

On installation, before creation of named “real person” Server administrator accounts, server setup occurs with the generic user account “serveradmin”. The initial password must be changed at first login.

6.2 Center administrator

Center administrators administer the XLeap Center “from within”. They have all privileges required for controlling the behavior of the XLeap Center within the fundamental configuration specified in the Server console. Their primary concerns include

- authentication requirements
- appearance (branding) of the XLeap Center
- limitations on other administrative roles
- assignment of administrative roles

Center administrators must have a clear understanding of the organization’s IT standards and operating procedures. This means that the role is often assumed by IT staff.

Center administrators, by definition, have the powers of

- User administrators, i.e. the privileges for managing user accounts
- Session administrators, i.e. the privileges for deleting and reassigning sessions

To help in the day-to-day operation of the XLeap Center, Center administrators can appoint other users to these roles.

Further, Center administrators can appoint other individuals or themselves as

- Template managers, i.e. users who manage session templates for compliance and best practice; Template managers need a Host license
- Subscription administrators, see below

The tasks and controls of the various administrative roles are explained in the “Center Administration Guide – XLeap In-house Server”.

Initial assignment. The initial Center administrator must be determined on purchase. The initial Center administrator is also the initial Subscription administrator.

6.3 Subscription administrator

Center administrators can appoint up to 3 Subscription administrators. While Center administrators can appoint themselves to this role, the role is often devolved to individuals of the user community rather than IT.

Subscription administrators are responsible for

- maintaining the Server and User subscriptions as required, mainly by coordinating the relevant purchase orders, renewals, and changes within the customer organization and between the customer and XLeap sales

- licensing named individuals as Host through the relevant Host subscription.

In large organizations with many licensed Hosts and multiple Hosts subscriptions for different departments or geographies, the licensing of new users and the un-licensing of those who leave the organization or move on to another role can become a daily task. Which is why Subscription administrators can

- purchase the required number of Host licenses through multiple rather than just one big Host subscription
- appoint up to 2 Licensors per Host subscription.

Example: By purchasing separate Host subscriptions for the Marketing, Sales and R&D departments, Subscription administrators could appoint 2 individuals from each of these departments as Licensors to take care of the day-to-day management of their respective subscriptions.

Reassignment of licenses is designed to help organizations deal with personnel changes. Licenses may not be reassigned to cover a larger number of individuals than paid for.

Appendix: Server deployment planning form

This planning form lists the decisions to be taken and the prerequisites for deploying an XLeap In-house Server on the Internet.

A.1. Server specs

Architecture: ☐ Intel 64 bit (required!)

RAM: _____ GB (recommended ≥ 8 GB, ≥ 16 GB for larger deployments)

Allocated storage: _____ GB (500 GB recommended)

Server location: _____

A.2. Server operating system and java

Operating system _____Release: _____

☐ OS supported by XLeap (c.f. section 1.2.1 Server software requirements)
☐ Windows Server has Java Runtime (any contemporary JRE) installed

A.3. Server access

☐ Root password requested
☐ Root password received: _____
☐ Root access tested
☐ File transfer possible
  ☐ Direct access to the machine
  ☐ File transfer via FTP
  ☐ File transfer via SSH/SCP
  ☐ Other: _____

A.4. Accessibility on the network

Allocation of IP addresses and DNS registration:

☐ Routable (public) IP address requested
☐ Public IP_____._____._____._____ allocated to the server
☐ Hostname: _____ (URL of XLeap Center)
☐ DNS registration requested
☐ Hostname available (tested!) as sub domain in the DNS
☐ Deployment with NAT
  If yes
  ☐ Private (NAT) IP address requested for the server

☐ Private IP_____._____._____._____ allocated to the server

Port mapping of XLeap Center application:

- ○ No port mapping (external port = listening port)
  - ☐ TCP 80 HTTP requested on firewall (if NAT is employed, including NAT)
  - ☐ TCP 443 HTTPS requested on firewall (if NAT is employed, including NAT)

or

- ○ Port mapping requested on firewall or server machine
  - ☐ HTTP external network port TCP 80 → application port TCP 8080 (if NAT is employed, including NAT)
  - ☐ HTTPS external network port TCP 443 → application port TCP 8443 (if NAT is employed, including NAT)

Server console ports:

Typically, the listening port of the Server console (Default: TCP 62701 HTTPS) need not be changed. Though configurable, there is usually no need to introduce complexities like mapping between external and listening port.

☐ Listening port of the Server console TCP _____ (Default: TCP 62701 HTTPS)

- ○ External port = listening port

or

- ○ External port TCP _____ (Port mapping)

Only if Server console is to be reached from the Intranet/Internet:

- ☐ Ports requested on firewall (if NAT, including NAT)
- ☐ Ports available (tested!) on firewall (if NAT, including NAT)

A.5. Database

- ○ Use embedded database for the XLeap Center

or

- ○ Use customer-installed database server

If yes,

- ☐ Database is supported by XLeap (c.f. section 1.2.1 Server software requirements)
- ☐ User and connection details received (username, password, IP, ports, schema, encryption etc.)

Note: XLeap Servers install with the embedded database Apache Derby. Migration to a 2nd-tier database server can only occur after successful installation.

A.6. Backup

The XLeap Server must be integrated into the data center's backup routine, for instance, by taking periodic snapshots of the server's file system.

☐ Server backup occurs by data center service: _____

- ☐ Inclusion requested
- ☐ Inclusion implemented / tested

A.7. Certificate for TLS-encryption of traffic

- ☐ Java keystore and authorized TLS certificate requested
- ☐ Keystore _____ available

  Password _____

If you are not familiar with TLS-keystores, download step-by-step guide 'Creating an authorized SSL certificate for XLeap'.

A.8. System email

The email service is required for sending passwords and notifications.

☐ User account for server requested on outgoing mail server (SMTP server, MTA)

Account information

Address: IP _____._____._____._____, Hostname _____

Port: _____

Username: _____

Password: _____

- O STARTTLS encryption of mail via STARTTLS command

or

- O SSL/TLS encryption of mail
- O SMTP server is reachable from XLeap Server (tested)

or

- O The XLeap Server can reach the SMTP server only via SOCKS proxy

  If yes
  - ☐ Account requested on SOCKS proxy
  - ☐ Account on SOCKS proxy created and tested

    Proxy Address: IP _____._____._____._____, or

Hostname _____ Port: _____

Username: _____

Password: _____

A.9. Outgoing HTTPS connections

The XLeap In-house Server requires an outgoing connection to the

- XLeap licensing system https://store.xleap.net
- Conferencing service https://session.voxeet.com (unless administratively disabled)
- SSO identity service (optional)

O The XLeap Server can establish TCP 443 HTTPS connections directly

or

O The XLeap Server establishes outgoing HTTPS connections via proxy

If yes

☐ Account requested on HTTPS proxy

☐ Account on HTTPS proxy created and tested

Proxy Address: IP _____._____._____._____,

Hostname _____ Port: _____

Username: _____

Password: _____

> *NOTE:* At the technical level, XLeap In-house Servers identify as "Internet Explorer 6". If your proxy restricts browsers that can use it, make sure that the so called "user agent" used by XLeap is listed:
>
> Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)

☐ User agent "Internet Explorer 6" is accepted by the proxy

A.10. Server administrators

List all persons to receive server administration privileges.

1. _____

2. _____

3. _____

A.12. Initial Center and Subscription administrator

Name the initial Center and Subscription administrator for the XLeap Center

1. _____