



## Privacy and Security in the Second Life Enterprise Beta

### Executive Summary

The Second Life Enterprise Beta (SL Enterprise Beta) enables you, as an enterprise or government institution, to run a complete 3D virtual world behind your organization's firewall. SL Enterprise Beta:

- Enables employees to interact, collaborate, create 3D content, and use 3D spaces via their avatars
- Gives you complete control over your virtual world, and keeps your private data securely behind your firewall
- Provides administrative tools that give you full control over user accounts, including access control

Because the SL Enterprise Beta system runs inside your network environment, behind your firewall, it can be just as secure as the rest of your network. Depending on your needs, you can configure SL Enterprise Beta access in three ways: to people exclusively within your network; to users within your network and to those outside of your network with VPN access, or to people both within and outside your network.

Additionally, SL Enterprise Beta provides a broad range of tools to maintain security, to set up private meetings with selected attendees, and to manage users.



Table of Contents	
Executive Summary	1
The Second Life Enterprise Beta System	3
Network Architecture	3
Management Tools	5
<b>User Management</b>	
<b>Region Management</b>	
<b>Upgrading, Scalability, and Extensibility</b>	
Second Life Enterprise Viewer Security	6
Data Security	6
Voice Security	6
<b>Group Voice Chat</b>	
Techniques and Best Practices	7
<b>User Credential Security</b>	
<b>Private Meetings</b>	
Integration and Interoperability	8
<b>Transferring Content</b>	
Technology Requirements	9
<b>Data Center and Network Requirements</b>	
<b>Network Bandwidth</b>	
<b>Desktop Requirements</b>	
Appendix I: Network Ports	10
<b>Second Life Enterprise Beta Server Ports</b>	
<b>Voice Server Ports</b>	
Appendix II: Glossary	10



## The Second Life Enterprise Beta System

The SL Enterprise Beta system includes all the necessary server hardware and software to run your business virtual world, including two server machines:

- **Second Life Enterprise Beta Server:** generates the 3D virtual world and its contents
- **Second Life Voice Server:** provides high-quality spatial voice chat for all users

Employees access the virtual world by running the Second Life Enterprise Viewer, a customized Second Life application for the SL Enterprise Beta-on their desktop system (Windows or Mac OS) and then connecting to the servers.

### Authentication and Authorization

Each user requires a user name and password to log in to the system. The web administration control panel (see Management tools) uses the same login credentials as the SL Enterprise Beta virtual world. Certain users have administrator privileges that give them special capabilities to manage the SL Enterprise Beta installation.

SL Enterprise Beta uses secure sockets layer (SSL) to encrypt connections to both the control panel and the authentication system. The servers can use either self-signed SSL certificates or certificates signed by your own certification authority.

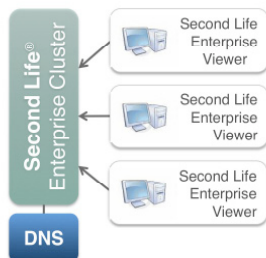
### Network Architecture

The Second Life Enterprise Beta runs behind your corporate firewall connected to your data center LAN in one of the following network configurations:

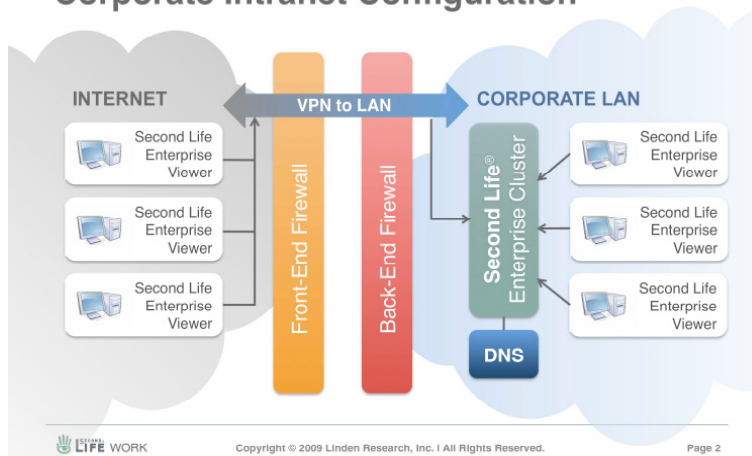
- **Isolated Configuration (Option 1):** Servers are accessible only to users on the local intranet. This is the most secure option, particularly suited to government and military applications.
- **Intranet Configuration (Option 2):** Servers are accessible to users on the local intranet and users on internet using a Virtual Private Network (VPN), if one is configured. The server cluster is installed within the inner network firewall. This option provides a good balance between security and accessibility, particularly if you have a VPN.
- **DMZ Configuration (Option 3):** Servers are accessible to authorized users on both the local intranet and on the internet, without VPN. The server cluster is installed between the outer and inner corporate firewalls, in the network "DMZ." This configuration provides the lowest level of security, but is appropriate when you want external users (customers, partners, or remote workers) to access the server without using a VPN.



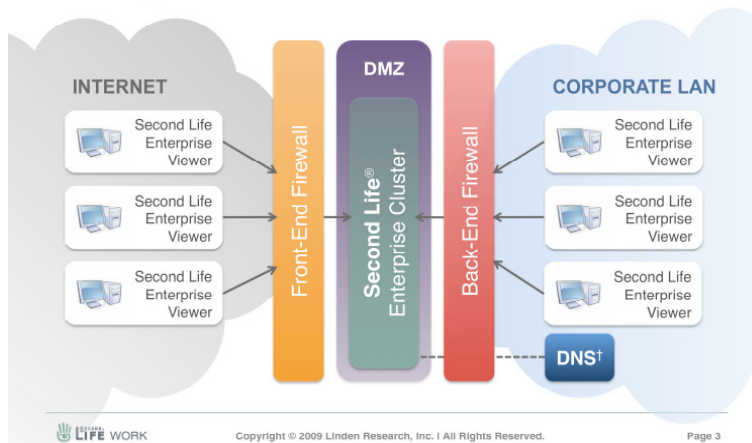
## Architecture: Option 1 Isolated Intranet Configuration



## Architecture: Option 2 Corporate Intranet Configuration



## Architecture: Option 3 Configuration with Servers in DMZ





## Management Tools

The Second Life Enterprise Beta solution includes three administrative tools:

- Web Control Panel - uses a secure HTTP connection over SSL and provides an easy-to-use graphical interface for all administration tasks.
- Command Line Interface Administration Tool (CLI Admin Tool) - a basic command-line tool for initial configuration.
- Inworld Administrator Features - includes “god tools” that an administrator can use to communicate with users, control user access, kick out users, and so on.

## User Management

Second Life Enterprise Beta administrators can easily:

- Create new user accounts, including avatar first name, last name, email address, password, and other details.
- Create many accounts “in bulk” by importing user data from a CSV file.
- Modify and delete user accounts at any time as needed.

To link user accounts to your Lightweight Directory Access Protocol (LDAP) database, simply specify your LDAP server when you initially configure Second Life Enterprise Beta. It will then respect user credentials in the LDAP database.

## Region Management

A Second Life region is a 256m x 256m area in the 3D virtual world, generated by a single simulator process or “sim.” SL Enterprise Beta provides extensive region management capabilities, including the ability to:

- View region status (running or stopped)
- Start and stop regions
- List all users currently in each region

## Upgrading, Scalability, and Extensibility

Second Life Enterprise Beta has a built-in upgrade facility, to enable you to easily upgrade the software and apply patches with the latest improvements and bug fixes.

By default, the SL Enterprise Beta comes with 7 pre-built regions: a 4-corners all-hands auditorium, 2 conference centers, a Space Station, and number of sandbox regions. Eight regions can run simultaneously, depending on the configuration. Expanding your SL Enterprise Beta to accommodate more regions is easy: simply purchase more simulator servers.



## Second Life Enterprise Viewer Security

The Second Life Enterprise Viewer (the client application) does not compromise users' computer security. The SL Enterprise Viewer has underlying security enhancements in addition to those of the standard Second Life Viewer application.

The only third-party application in the SL Enterprise Viewer is the voice chat client that is integrated by Linden Lab. The SL Enterprise Viewer application does not have a plug-in architecture, which might make it vulnerable to security exploits. It can also launch the user's default web browser, but it does not have the capability to launch other applications.

To speed the display of graphic content, the SL Enterprise Viewer locally caches some content such as texture data. The cache is unencrypted, but the cached data does not include account information; it only contains object information (for inworld inventory and assets). It does cache login credentials locally when the user specifically checks the "Remember password" box on the login screen.

If the user checks the "Remember password" box on the login screen, SL Enterprise Viewer caches login credentials locally to disk in an encrypted form. When using LDAP authentication, it saves LDAP account passwords in an encrypted store. SL Enterprise Viewer also saves native Second Life Enterprise Beta account authentication tokens derived from the password, but not the actual passwords.

SL Enterprise Viewer is susceptible to man-in-the-middle attacks only when the attacker is on the same network hub or the user is on an insecure WiFi network.

## Data Security

Because the SL Enterprise Beta system runs inside your corporate firewall, it has the same level of security as that of the rest of your network. All confidential and proprietary information and network traffic remains solely within your corporate network. Exception: when using the DMZ network configuration (illustrated in Fig. 3), users outside your network will be able to access your SL Enterprise Beta system.

Second Life Enterprise Beta provides manual and automated backup of all objects, land, and avatars. You can restore content at any point if necessary. SL Enterprise Beta machines provide disk redundancy through RAIDs.



## Voice Security

The Second Life Enterprise Beta includes a voice chat server that provides a Voice Over Internet Protocol (VOIP) system for public spatial, private spatial, group, and person-to-person voice chat. Because the voice server resides along with the rest of the SL Enterprise Beta system in your data center, it and the voice data it processes are just as secure as the rest of your internal servers.

You can always monitor the speakers list in a voice chat to see who inworld is able to hear your conversation. Anyone who can hear your conversation shows up in the speakers list, so you are alerted when a private conversation or meeting is being monitored by another user.

### Group Voice Chat

To ensure private voice communication among multiple people, simply create a group (or use an existing group). Every group automatically has its own group chat channel. When you use a group chat channel, only people in the group are able to listen to the conversation.

A person in a group can start a private group chat with a few mouse clicks. Then, other members of the group can similarly join (and leave) the chat session as they wish. Group chat is not spatial, that is, it doesn't depend on your inworld location: everyone in the group who has elected to join the chat session can hear the other participants, regardless of their inworld location.

## Techniques and Best Practices

### User Credential Security

User names and passwords enable secure access to SL Enterprise Beta. It is important to maintain the integrity and confidentiality of these credentials, just as it is for any network login credentials. For example, ensure that administrators promptly revoke terminated employees' login privileges; SL Enterprise Beta administration tools make this easy.

If you are using the DMZ network configuration (illustrated in Fig. 3), you must take special care to maintain the security of login credentials, since users outside your corporate network will be able to login.



### Private Meetings

Even behind your corporate firewall, you may want to have meetings with restricted attendance that are not accessible to uninvited employees. You can handle such situations with two Second Life Enterprise Beta features: groups and restricted parcels.

- A Second Life *group* is a set of two or more users. Groups can be open (anyone can join) or closed (join by invitation only). Groups have a variety of sophisticated features, including the ability to assign roles with special abilities (for example, the ability to send notices to all group members). Groups can also conduct voice chat and text chat over a private group channel, accessible only to group members.
- A *parcel* is an a demarcated area of virtual land; administrators can assign ownership of parcels to individuals or groups. The administrator or owner can then easily create a private space for such meetings by restricting access to the parcel to the group or selected individuals. Administrators can handle such tasks, or delegate such responsibilities to individuals.

For example, you might create a user group called “Executives,” and add all members of the executive staff to that group. Then you could secure a “boardroom” meeting space by restricting access to the parcel containing the meeting area to the “Executives” group. Then only members of the executive staff could enter that parcel and listen to voice chat conducted over the executive group channel.

There is one possible security concern on properly secured parcel: A user could bring an untrustworthy object or attachment (for example, hair, a wristwatch, or a vehicle) into the space could potentially contain a Linden Scripting Language (LSL) script that records text chat or local avatar and object names. An authorized user would have to create or bring such an item inworld, so this concern is analogous to that of employees bringing “bugs” or listening devices into a real-world meeting.

Note that LSL scripts cannot:

- View or record instant messages (including group IM) unless the chat targets the scripted object.
- Listen to or record voice communication, or media streams
- Directly capture visual content such as objects or textures.



## Integration and Interoperability

Your Second Life Enterprise Beta environment is totally separate and disconnected from the public Second Life environment. This provides security and privacy, and gives you total control over who can access your SL Enterprise Beta and the 3D virtual content.

### Transferring Content

If you have intellectual property rights to existing Second Life content (regions, structures, objects, and so on), you can use the content in your SL Enterprise Beta environment. Linden Lab will transfer the content to your SL Enterprise Beta installation upon request as long as you provide written assurance that you own (or have the right to transfer) the intellectual property rights to the content.

Additionally, Linden Lab may offer Second Life content creators the opportunity to sell their content to SL Enterprise Beta customers. You will be able to transfer content purchased from Resident content creators who have made it available for SL Enterprise Beta environments. You will be able to move the content to your SL Enterprise Beta environment only if the creator has explicitly given permission to do so.

## Technology Requirements

Second Life Enterprise Beta is designed specifically to run within a corporate or organizational firewall installed in a standard corporate data center.

### Data Center and Network Requirements

Second Life Enterprise Beta requires a data center with standard amenities such as a server-class cooling system. In addition to a firewall that provides network security, SL Enterprise Beta requires access to a DNS server, even for the isolated network configuration. You must open a small set of TCP and UDP ports to the servers, as described in Appendix I.

To avoid loss of service and data due to power outages, use an uninterruptible power supply (UPS). Power interruptions can cause total loss of service and loss of any data created within the last hour.

The Second Life Enterprise Beta machines are rack-mounted, and the installation requires 2us of rack space. The SL and voice servers require a 410W power supply.

### Network Bandwidth

Second Life Enterprise Beta supports up to 800 concurrent users with optimal performance at 400 concurrent users or less.



Average peak downstream bandwidth required is 100 Kb/s per concurrent user. Thus, 100 concurrent users would require a network capacity of  $100 \text{ Kb/s} \times 100 = 10 \text{ Mb/s}$ . While individual users may peak above 100 Kb/s, not all users will peak at the same time; so 100 Kb/s per concurrent user is a good rule of thumb for bandwidth planning.

NOTE: In general, the upstream bandwidth requirements are much lower than downstream bandwidth requirement.

### Desktop Requirements

The Second Life Enterprise Viewer runs On Windows XP and Vista, Mac OS, and Linux desktop systems. For more information, see Second Life System Requirements at (<http://secondlife.com/support/sysreqs.php>).

## Appendix I: Network Ports

### Second Life Enterprise Beta Server Ports

TCP	UDP
80	12043
443	13000-13050
12035	

### Voice Server Ports

TCP	UDP
12000	12000
21002	21002
19000	

## Appendix II: Glossary

**Chat Channel** : All voice communication in Second Life occurs on a “channel.” Spatial chat (from nearby speakers) occurs on channel zero; you can also set up individual and group chat channels. Multiple channels can co-exist, but you can participate in only one channel at a time.

**DMZ (De-Militarized Zone)**: A physical or logical subnetwork that exposes an organization’s external services to the internet. A DMZ adds an additional security layer to a LAN: an external attacker can access only hosts in the DMZ, rather than the whole network.



**INWORLD:** Within the 3D virtual world of Second Life or Second Life Enterprise Beta.

**LAN (Local Area Network):** A computer network covering a small physical area, often using Ethernet cabling and/or Wi-Fi wireless transmission.

**LSL (Linden Scripting Language):** The programming language used to control the behavior of inworld objects. LSL has syntax similar to C. SL servers (sims), not the client (Viewer), interpret and execute LSL. However, the Viewer provides a full-featured LSL editor.

**Region:** A named 256m x 256m virtual area hosted by a single simulator process.

**Second Life Enterprise Viewer:** The enterprise version of the Second Life Viewer, the Second Life client software.

**Sim (Simulator):** Can refer to both the server machine simulating one or more regions ("sim host") and to the processes running on the server machines ("sim process"). In common usage, "sim" may also be used to mean a Second Life region.

**SSH (Secure Shell):** A network protocol for shell (command-line) access that provides for secure data exchange between user and a remote host.

**TCP (Transmission Control Protocol):** A standard network protocol that provides reliable, ordered delivery of data from one computer to another.

**UDP (User Datagram Protocol):** A standard network protocol useful for servers that answer small queries from huge numbers of clients. UDP is compatible with packet broadcast (sending to all on local network) and multicasting (send to all subscribers).

**VOIP (Voice Over Internet Protocol):** A general term for transmission technologies for voice communications over IP networks such as the internet.

**VPN (Virtual Private Network):** A private network that uses a public network (usually the internet) to connect remote sites or users together. A VPN provides secure access to private network resources without the expense of private network hardware.



### **About the Second Life, by Linden Lab**

Developed and launched by Linden Lab in 2003, Second Life is the world's leading 3D virtual world environment. It enables its users - known as Residents - to create content, interact with others, launch businesses, collaborate and educate. With a thriving inworld economy that saw over \$360 million USD transacted in 2008, and a broad user base that includes everyone from consumers and educators to medical researchers and large enterprises, Second Life has become one of the largest hubs of user-generated content (UGC) in the world.

### **For More Information**

visit our website:

<http://work.secondlife.com>

visit our land store:

<http://secondlife.com/land/>

visit our blog:

[http://blogs.secondlife.com/  
community/workinginworld](http://blogs.secondlife.com/community/workinginworld)

follow us on Twitter:

<http://twitter.com/workinginworld>

email: [business@lindenlab.com](mailto:business@lindenlab.com)

Linden Lab, founded in 1999 by Chairman of the Board Philip Rosedale and headquartered in San Francisco, develops revolutionary, immersive technologies that change the way people communicate, interact, learn and create. Privately held and profitable, Linden Lab is led by CEO Mark Kingdon, and has more than 300 employees across the U.S., Europe, and Asia.

### **Linden Lab**

945 Battery Street

San Francisco, CA 94111

Phone: (415) 243-9000

Fax: (415) 243-9045

Copyright © 2009 Linden Research, Inc. All rights reserved. Linden Lab, Second Life, Second Life Grid and the Second Life and Linden Lab logos are registered trademarks of Linden Research, Inc. .