



White paper for version 3.3.0, 1st ed.

2011-12-20

Cendio AB
Wallenbergs gata 4
SE-583 30 LINKÖPING

Table of Contents

Preface.....	3
Overview.....	3
Flexible Architecture.....	3
Compatible with Directory Services.....	3
Compatible with File Servers.....	4
Clustering.....	4
High Availability Through Fault Tolerance.....	4
Two-tier Load Balancing.....	4
Clients.....	4
Built-in End-to-End VPN.....	4
Security	5
Encryption	5
Secure Against "Man-In-The-Middle" Attacks.....	5
One-Time Passwords.....	5
Smart Cards.....	5
Installation.....	5
Novell Configurator.....	5
Usage.....	5
Open Source Software.....	5
Desktop Publishing.....	6
Virtual Desktop Infrastructure, VDI.....	6
Application Publishing.....	7
Session Based.....	7
Web and Portal Integration.....	7
Single Sign-On.....	7
Cut and Paste.....	7
Printer Management.....	7
Support for Local Drives.....	8
Serial Port Support.....	8
Sound Support.....	8
Greater Control.....	8
ThinLinc Administration using Web Interface.....	8
Server System Requirements.....	9
ThinLinc has been tested on the following platforms:.....	10
Support for the Following Application Types.....	10
Support for the Following Authentication Mechanisms	10
Client Platforms – General Operating Systems.....	10
Client Platforms – Thin Terminals.....	10
The Structure of ThinLinc.....	11
Proprietary Software.....	11
VSM.....	11
Open Source Software.....	11
TigerVNC.....	11
OpenSSH.....	12
VirtualGL.....	12
rdesktop.....	12
Add-on Products.....	12
CrossOver Professional.....	12
NordicEdge OTP.....	12

Preface

This document describes ThinLinc®, version 3.3.0, from Cendio AB. The purpose of the document is to give the reader more information about the product and its properties. ThinLinc is delivered with extensive documentation for further reading.

Overview

ThinLinc is Cendio's product for server based computing. ThinLinc is software used to centralize applications by the use of Server Based Computing; a so-called "terminal server".

The product is largely based on Open Source Software. This has contributed to faster development times, and also to making the product very robust, and at the same time adaptable. The use of Open Source Software in the products also means that many functions – which are delivered as add-ons in other products – are part of ThinLinc from the start: encryption, single sign-on, clustering, advanced printer management, and integration between different systems and services.

Flexible Architecture

Most organizations have different needs and, consequently, very different systems solutions. That is why ThinLinc's system architecture is adapted to allow the existing infrastructure to be used alongside the new architecture. ThinLinc can be put into operation in parallel with the existing environments and can even be integrated with them, thereby enabling a step-by-step migration to a new platform.

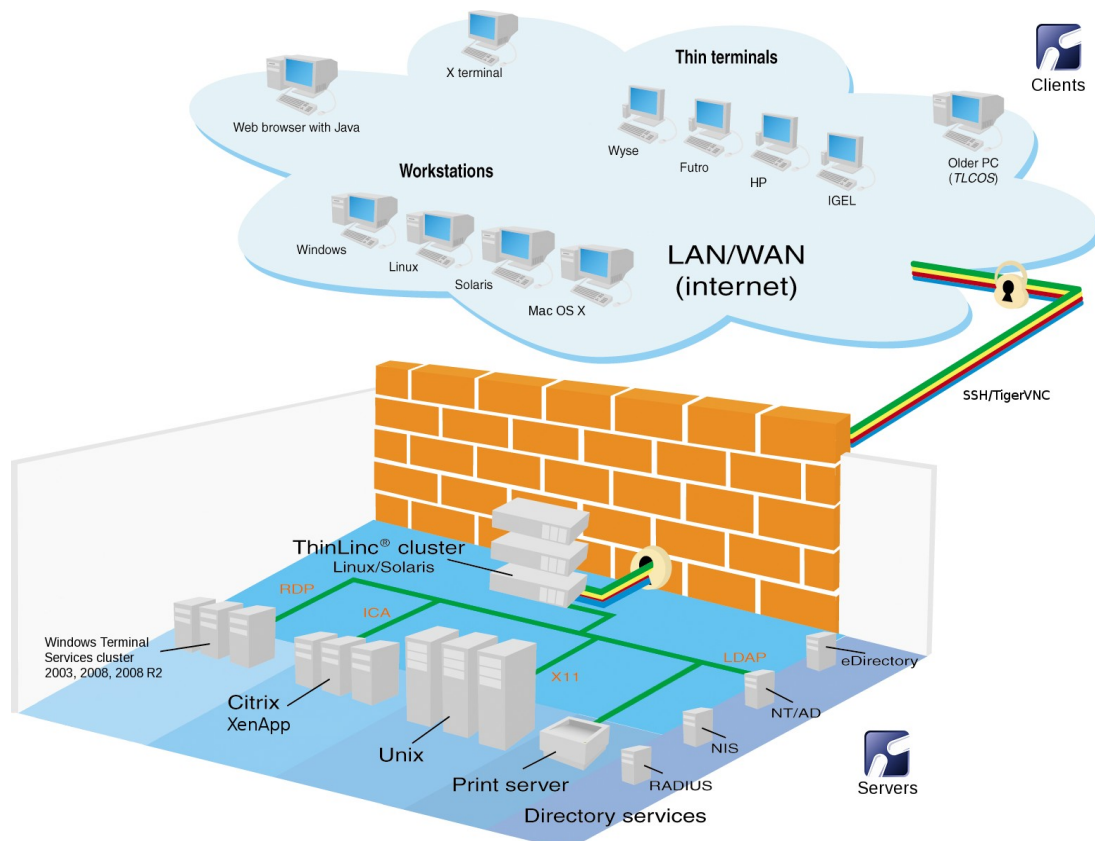


Illustration 1: The system architecture as seen from the data center.

Compatible with Directory Services

An important part of the existing server environment is often the directory service. ThinLinc can use, for example, eDirectory, Active Directory or NIS.

Compatible with File Servers

ThinLinc can mount home directories and other file systems from Windows (via CIFS), Unix and Linux (via NFS) and Novell (via NFS and NCP).

Clustering

For larger systems, clustering is recommended. ThinLinc can cluster in two different ways at the same time: load balancing and high availability (HA) clustering.

High Availability Through Fault Tolerance

When using Server Based Computing, it is important that the system has high availability, since everyone connected to the system is affected by a system stop. In a system with two machines, one is the "primary" and the other is the "secondary". In the cluster, the secondary can take over the primary's job in case of a problem. ThinLinc contains functions for automatic fail-over in case of a malfunction.

Two-tier Load Balancing

ThinLinc also features load balancing. This means that the servers will be equally loaded, as much as possible. When a user logs on he/she is assigned to the server with the least load (as established by pre-defined criteria.) In ThinLinc there are built-in load balancing agents which not only handle the terminal servers, but also Windows servers with Terminal Services. This means that load balancing is taking place on two levels. Application servers with Windows Terminal Services can also be freely clustered in the same group, regardless of whether the version is Windows Server 2000, 2003 or 2008.

Clients

A system for Server Based Computing should be accessible to different kinds of workstations and terminals. The following types of terminals can access ThinLinc:

- *Fat client*: a workstation.
- *Thin terminal*: small diskless and fan-less hardware with ThinLinc client installed.
- *Thinned client*: older computer which is used as a "thin" terminal. For this purpose, Cendio has created the *ThinLinc Client Operating System* (TLCOS), a tailored Linux distribution which makes a thin terminal out of an older PC. Another possibility is to use the packaging of *ThinStation* (<http://www.thinstation.org/>) that does the same. The most important difference is that TLCOS is installed on the harddisk and ThinStation boots from the network.
- *X terminal*: Specialized client. These require certain special solutions in the server, and some of the advantages of ThinLinc are diminished, for instance the low bandwidth requirement.
- *Web browser client*: for web browsers with Java.

To see what the clients require, see also the sections "Hardware requirements" and "Client requirements" below.

Built-in End-to-End VPN

SSH is delivered with the client at no extra cost. The architecture permits a very secure solution to be constructed for external access or for working remotely. ThinLinc can entirely or partly replace the need for VPN in a company or organization. The system also works together with existing VPN systems.

There are three important differences between ThinLinc and an ordinary VPN:

1. The connection terminates in the ThinLinc server, not in the firewall. For large networks with a central firewall, this can make a decisive difference.
2. For VPN with IPSec, all network connections from the client are often locked, which means that all traffic has to pass through the firewall multiple times. With ThinLinc, the user can, for instance, browse the web as usual, without the tunnel being affected.
3. The installation of ThinLinc is very simple and doesn't require any advanced setup by the user.

This "end-to-end" VPN is used for all functionality in ThinLinc.

Security

Encryption

ThinLinc uses SSH to encrypt the connection between the terminal server and the clients. SSH can use a number of encryption algorithms, including AES, "Advanced Encryption Standard", which permits up to 256 bit symmetric encryption.

Secure Against "Man-In-The-Middle" Attacks

The ThinLinc client requires that the user accepts the server from which the session is run. Any changes on the server or an attack causes the client to automatically issue a warning and disconnect the session.

One-Time Passwords

From ThinLinc version 1.4.0, One-Time Passwords are supported. Cendio has created this feature in cooperation with the Swedish company Nordic Edge AB and their product OTP Server. For more information about Nordic Edge AB, see: <http://www.nordicedge.se/>. ThinLinc also has support for authentication using RSA SecurID with a token.

Smart Cards

From version 2.0.0, ThinLinc has support for smart cards. The support comes in two forms: The first is support for smart card authentication using the PKCS#15 standard. The second is support for applications running on the ThinLinc server, or application servers with Windows Terminal Services, using the PC/SC standard.

Single Sign-On works with smart cards when using either Novell eDirectory or MS Active Directory as a directory server.

From version 2.1.0, ThinLinc also supports automatic login when a smart card is inserted, so that you can carry your session with you.

Installation

Installation of a ThinLinc server is very simple. Great care has been taken to ensure that the installation and configuration is as quick, easy and foolproof as possible.

The ThinLinc installer can be run either in a graphical mode or a text mode. In addition to the installer, there is a setup program that is run automatically by the installer. This setup program

sets up the surrounding Linux environment to fit ThinLinc, for example installing printer queues for local and nearest printer, etc.

Novell Configurator

An important feature that makes integration into a Novell network simpler is the *Novell Configurator*. When ThinLinc is installed in an environment with Novell eDirectory as a directory solution, a number of steps have to be performed in order to ensure interoperability between ThinLinc and eDirectory. The Novell Configurator aids in this configuration, in most cases making the configuration as easy as clicking a single button.

Usage

Open Source Software

ThinLinc is largely based on Open Source Software, which has meant lower costs for development and testing. Open Source Software is a term used to describe software for which the source code is available to anyone, and for which the license doesn't restrict its use, modification and redistribution.

All software which is part of the product has a good reputation and is thoroughly tested, with many years of development and use. This has facilitated the quality assurance of ThinLinc.

Desktop Publishing

The user can use a published desktop running on the ThinLinc server. The operating system and applications running on the server will have access to local resources on the client, such as the hard disk, USB memory sticks, etc. In most important aspects the user will feel as if the desktop is running locally. Since ThinLinc allows applications from different operating systems to coexist, not all applications need to come from just one operating system. Instead, the users are free to use the applications which suit them best.

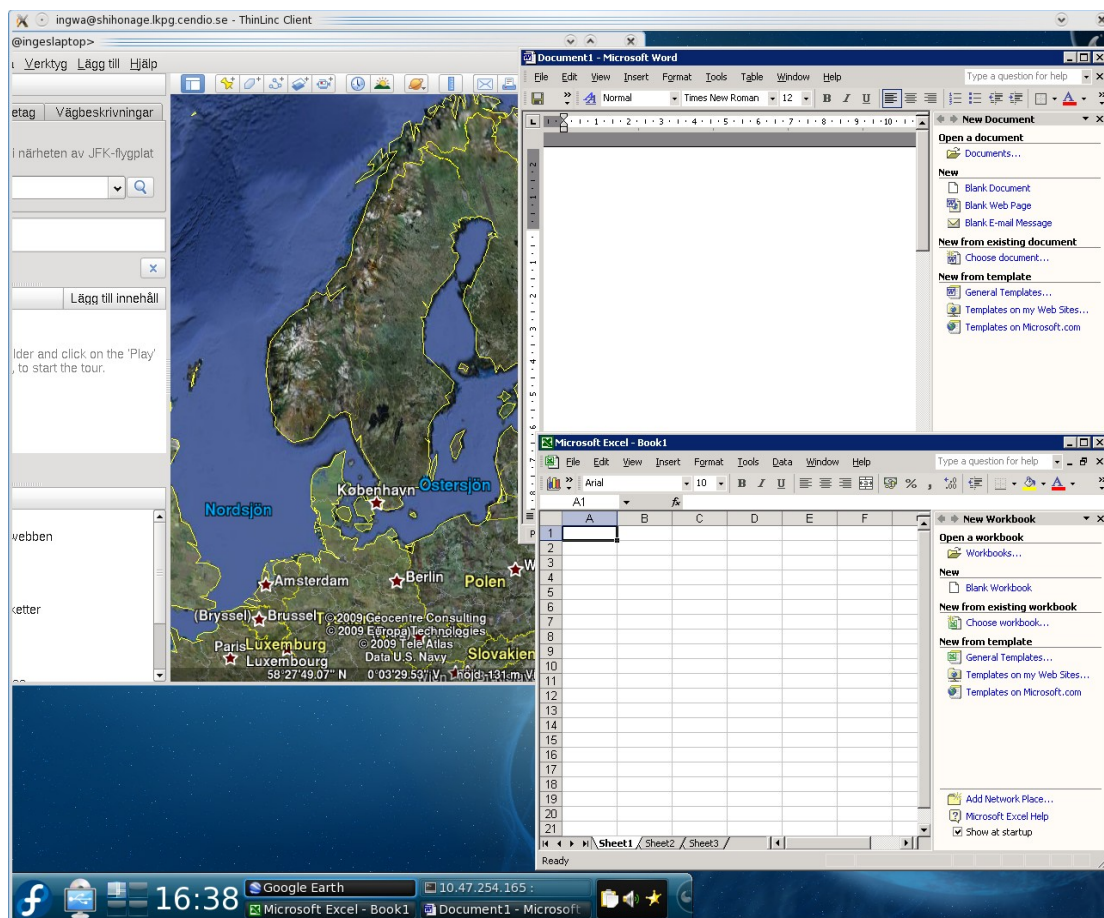


Illustration 2: Example of how applications from different operating systems can coexist in ThinLinc. Note how ThinLinc can use OpenGL and therefore run Google Earth.

ThinLinc makes it possible to use a Linux desktop with applications which normally require Windows. Cendio cooperates with Codeweavers Inc. and their product *CrossOver Professional* to make it possible to run applications directly on the ThinLinc server without the need for any Windows Terminal Server. For more information about CrossOver, see: <http://www.codeweavers.com/>

If you want to run applications that only work on Windows, you can do this seamlessly by using the ThinLinc feature SeamlessRDP. This feature lets a Windows application that is running on Windows Terminal Services open its windows on the Linux desktop as if they were running directly under Linux or CrossOver.

The change to a Linux desktop can be deterring for some users. By adapting the desktop to, for instance, look like Windows, it is easier to convince most people of the benefits the change brings.

Virtual Desktop Infrastructure, VDI

Thinlinc has built-in support for VDI brokerage. ThinLinc can act as a front-end to virtual machines just like it can act as a front-end to sessions on a terminal server as described above.

ThinLinc can interact with a virtual machine infrastructure such as VMware Virtual Infrastructure and let machines boot automatically when the user logs in. In contrast to most other VDI brokers, ThinLinc lets the user enjoy full support for local devices, such as double-directed sound, local storage devices, serial ports and the local printer.

Since version 3.2.0, ThinLinc also features support for using VirtualBox as a VDI backend. VirtualBox works well with VirtualGL, providing hardware accelerated OpenGL graphics to virtual machines.

Application Publishing

Starting with version 2.0.0, ThinLinc also supports basic publishing of single applications. There is no limit on the number of applications that can be published to the same user, and they can be running on different operating systems in the same manner as described above.

Session Based

ThinLinc is session based, which means that the users can move between different client computers without changing the session. The server keeps track of all sessions, so if the user wants to change clients, or if the client computer crashes, then the session is saved and work can resume on any other client.

A "session" is a single user's desktop from when it is started to when it is closed. If the user just turns off the client instead of shutting down the desktop, the session is still running on the server. The next time the user starts a client and logs in, the session is just as it was when it was left – the cursor is even in the same place.

The time that a session is kept alive can be configured as needed.

Web and Portal Integration

ThinLinc is prepared to be run through a web portal. This means that the user can start any type of session (desktop or application) by clicking on a web link in a web browser. If the native client is not installed, a signed Java applet guides the user through the installation. The web browser integration is designed to be platform and browser independent.

Single Sign-On is available when used with products such as Portwise (<http://www.portwise.com/>).

Single Sign-On

ThinLinc contains a feature for so-called "Single Sign-On" into a number of environments. This feature lets the ThinLinc user connect to external applications or even desktops from these environments.

At this point, ThinLinc supports Single Sign-on to: Windows Terminal Services 2000, 2003 and 2008, Citrix ICA, all UNIX derivatives via SSH, and the Novell client. It is also available for authentication using smart cards.

Cut and Paste

ThinLinc supports "cut and paste" between different application servers, for instance between applications on Windows and Linux.

So far, only text can be handled.

Printer Management

With the help of CUPS (Common Unix Printing System) ThinLinc offers powerful support for printing. First of all, ThinLinc supports local printers installed on the client. The print jobs to this queue are transferred as PDF to save bandwidth. However, there is also support for raw print jobs that can be sent to special types of printers such as EAN printers or receipt printers.

There is also a special print queue which goes to the "nearest printer", i.e. the printer which has been set to be the one closest to the terminal from which the user logged in.

From 2.0.0, the new "Printer Access Control" feature makes it possible to restrict access to

certain print queues based on the connecting terminal. The user only sees the printers which are available from the location of the terminal.

Support for Local Drives

ThinLinc supports so called "local drives". Hard disks, disk drives, CD-ROMs and other storage media (for instance certain digital cameras, USB memory sticks, etc.) on the client can be accessed from the server and can be used by applications running through ThinLinc.

Serial Port Support

Through a so called "virtual serial port", it is possible to connect peripherals using the serial port for communication. This makes it possible to synchronize PDAs, or use other units which communicate through the serial port. ThinLinc supports two simultaneous serial ports.

Sound Support

ThinLinc supports sound from applications running on the ThinLinc server machine as well as from Windows Terminal Server via RDP. It uses a standard method for network transported sound built on PulseAudio, although software that uses the previous technology, Esound, can still be used. Note that ThinLinc supports two-way sound fully, which means that a microphone can be used with software that is running under Linux or CrossOver. Programs that run under Windows Terminal Services without ThinLinc cannot do this, since Microsoft RDP does not support it.

Greater Control

ThinLinc can be adapted to the work methods used in different groups. This makes it possible to take into account the needs and methods for different user groups and, in this way, increase productivity, while also getting the gains from rationalizations.

In the Thinlinc program packages, there are tools for creating different kinds of user groups and specifying which information and which applications each of them should have access to. With the *ThinLinc Desktop Customizer*, the desktop can be tailored to the needs of different groups. Which desktop and which "start menu" you get when you log in is determined by which group you belong to, your user id or profile. The Desktop Customizer works with the user environments KDE and Gnome.

The *ThinLinc Client Customizer* tool is used to pre-configure the client software with specific settings, for instance the server name or port for ThinLinc. These clients can then be deployed on a large scale without the need for any further manual configuration.

ThinLinc Administration using Web Interface

For administrators who are inexperienced with Linux, ThinLinc configuration and performance monitoring can be performed with a brand new, easy-to-use web interface.



Illustration 3: The web administration interface to ThinLinc.

Server System Requirements

Estimation of memory and processor power needs is based on the x86 architecture.

- A 32-bit, LSB-compliant Linux distribution, based on glibc 2.3.4 or greater, with RPM or dpkg support. An i686 (or compatible) CPU with MMX and SSE support
- or
- A 64-bit, LSB-compliant Linux distribution, based on glibc 2.5.1 or greater, with RPM or dpkg support. An x86_64 (or compatible) CPU
- or
- Sun Solaris® 10
-
- GLib 2.x
 - Python 2.3 or newer 2.X version
 - PyGTK 2.4.0 or newer
 - python-ldap (only for eDirectory integration)
 - CUPS (Common UNIX Printing System) (only when local or "nearest" printer is used)
 - A web server with support for SSL and CGI scripts (only required when using Browser Clients)
 - Hard disk: 100 MiB free hard disk space
 - CPU:
 - 50-100 MHz per active session (only if using RDP)
 - 150-300 MHz per active session (for desktops from Linux/UNIX with typical mix of applications)
 - 0.6-0.8 CPU cores per active 3D session (this figure is highly application dependent)

and should serve only as a starting point for further analysis)

- RAM: 128 MiB for the base system, plus:
 - 10-20 MiB RAM per active user session (only Windows and RDP) or
 - 100-150 MiB RAM per active user session (desktops from Linux/UNIX with typical mix of applications)
- GPU: For 3D applications, a 3D graphics accelerator is required in the ThinLinc server machine (examples: nVidia Quadro FX, ATI FirePro)
 - Depending on the characteristics of the 3D applications that will be run, as many as 8 users may be able to share a typical GPU. Some more demanding 3D applications may require as few as 1-2 users per GPU.

ThinLinc has been tested on the following platforms:

- Red Hat Enterprise Linux 6 (64-bit)
- Mandriva Enterprise Server 5.2 (64-bit)
- SUSE Linux Enterprise Desktop 11 SP1 (R) (64-bit)
- Ubuntu 11.10 (64-bit)
- Sun Solaris 10

Support for the Following Application Types

- Microsoft Windows (XP, Terminal Server or Citrix MetaFrame)
- UNIX (X11 protocol)
- Linux (X11 protocol)
- HTML
- Java

Support for the Following Authentication Mechanisms

- LDAPv3
- Novell eDirectory
- NIS
- Microsoft Active Directory
- UNIX passwords
- RSA SecurID
- HTTP, HTTPS
- One time passwords using Nordic Edge OTP
- All PAM based authentications, except for one-time passwords which require challenge-response.

Client Platforms – General Operating Systems

- Windows clients: Windows XP, XP Embedded, 2003, Vista, 2008, Windows 7 and 2008 R2
- Linux clients (including TLCOS):
 - Linux with GLIBC 2.3.4 or newer,
 - Hardware requirements: Pentium (i686 with MMX) or compatible CPU with 32 MiB RAM
- Mac OS X clients: Mac OS X version 10.4 or later on Intel platforms
- Solaris clients: Sun Solaris 8 or later on UltraSPARC processors
- Java client: Web browser which supports SSL. Java 1.4.2 or later is needed.

Client Platforms – Thin Terminals

- eLux based (Fujitsu Siemens Futro, et al.)
- IGEL
- Wyse's Linux based terminals
- Tecnoworlds Linux based terminals with Blanes
- Hewlett-Packard t5000 terminals
- Connec EZ800

The Structure of ThinLinc

ThinLinc is a framework which, to a large extent, uses Open Source Software. Cendio takes full responsibility for the programs which are part of the product, and in several cases we help develop the code in the open source projects.

Proprietary Software

At this time, ThinLinc partly contains proprietary software (also called closed source software), including, among others VSM. The system is built so that most of the Open Source software can be replaced with proprietary software, if the need should arise. The licenses for ThinLinc at large and the proprietary components are found at <http://www.cendio.com/legal/eula>.

VSM

VSM is the main framework in ThinLinc and is developed by Cendio. VSM stands for *VNC Session Manager*. VSM has other tasks than managing sessions, though. Among these are:

- Verifying and authenticating logins for single sign-on
- Starting sessions after authentication
- Supervising active sessions
- Load balancing
- Supervising the system performance
- Managing high availability clustering
- Interfacing between the different programs

Open Source Software

To see a list of the open source software which is part of the ThinLinc package under a free license, see <http://www.cendio.com/legal/oss>. Below is some information about the software that is part of or can be used with ThinLinc.

TigerVNC

The graphical information is sent between the server and the client using an optimized VNC protocol.

VNC stands for "Virtual Network Computing" and is a system for remotely displaying and interacting with a desktop running on another computer. VNC was developed by AT&T Laboratories in Cambridge. It is flexible with regards to, for instance, screen resolution and supports color depths up to 32 bits per pixel.

TigerVNC is an enhancement of VNC that is optimized for slow connections and high-performance graphics needs like real-time video and 3D applications. Even if the connection is slow, you can work in real time with the help of TigerVNC. On faster networks you can watch full-screen videos in real time with good quality. TigerVNC is free, compatible with VNC and is developed by Cendio and the Open Source community. See: <http://www.tigervnc.org/>

TigerVNC works well with VirtualGL, which makes it possible to run OpenGL based applications, such as CAD applications and Google Earth, in a ThinLinc session. All sessions on the server share one or more graphics processing units (GPUs), thus adding hardware-accelerated 3D rendering to thin client sessions.

TigerVNC supports many modern X extensions, such as RandR, which makes it possible to change the size of the session in real time without having to create a new session when you

move it to a terminal with another size.

ThinLinc uses Xvnc to assemble a "virtual desktop" with the different applications, which are run on the application servers, and then sends images of changed portions of the desktop to the client.

OpenSSH

The information is encrypted using OpenSSH, which is a free program that supports both SSH and SSH2. SSH supports a number of different encryption algorithms, like AES-128, AES-192, AES-256, DES, 3DES, Blowfish, CAST and ARCFOUR. Data sent between the terminal server and the clients can be encrypted with up to 256 bit encryption, but it is also possible to select a simpler encryption which requires less processor power if the security demands are not that high. See: <http://www.openssh.org/>

Encryption	AES (Rijndael)	BlowFish	Cast128	Arcfour	3DES
Patented	No	No	No	No	No
Number of bits	128, 192 & 256	Up to 448	Up to 128	Up to 128	168

VirtualGL

VirtualGL is a tool for virtualizing hardware-accelerated 3D graphics. VirtualGL intercepts 3D function calls from a 3D application running on a UNIX or Linux server and redirects these calls to a graphics processing unit (GPU), then reads back the rendered image from the graphics card and draws it into an X window.

Thus, VirtualGL enables the application to use hardware-accelerated 3D graphics even if the X server does not support it. Since VNC servers do not support hardware-accelerated 3D, VirtualGL is used to give TigerVNC hardware-accelerated 3D capabilities. The combination of VirtualGL and TigerVNC provides a fully virtualized 2D and 3D display environment, capable of excellent levels of performance even on full-screen 3D applications.

rdesktop

To run Windows programs you generally need a *Windows Terminal Server*. The communication between the application server and the terminal server uses the Remote Desktop Protocol (RDP) and the *rdesktop* application. *rdesktop* is an open source client software package for RDP (RDP is the protocol used by Windows Terminal Services). See <http://www.rdesktop.org/>

Add-on Products

Cendio has strategic partnerships with a number of companies that deliver products that add value to ThinLinc in various ways. A strategic partnership means that Cendio takes the responsibility that the products work together with every new version of ThinLinc and for documenting how to use the products together.

CrossOver Professional

ThinLinc can today be used on the Linux and Solaris platforms. Many customers that use Windows based software want to continue doing this even after they switch to ThinLinc. There are two ways of doing this:

1. Connect to one or more windows servers using Windows Terminal Services.
2. Use a Windows emulator like Wine or CrossOver (Linux only)

Cendio has a strategic partnership with Code Weavers Inc (<http://www.codeweavers.com>), a

company that delivers *CrossOver*. *CrossOver* is middleware that makes it possible to run Windows applications on the Linux platform. Cendio has been working actively with Code Weavers to adapt *CrossOver* to a terminal server environment. Among other things, the sound support has been adapted and documented, but also the support for centralized installation and configuration has been improved through this partnership.

Today, Cendio is the general agent and distributor of *CrossOver* for the Nordic market.

NordicEdge OTP

NordicEdge AB (<http://www.nordicedge.se>) is a vendor that delivers solutions for improved security, including solutions for efficient handling of one time passwords. Cendio has adapted the ThinLinc server and client software to be integrated with the NordicEdge One Time Password Server. This software delivers one time passwords through SMS to the user's mobile phone and is a very common system in Sweden today, especially within the public sector.