

Overview

Enexity's SecureLink Virtual Support Network enables on-demand network connectivity between secure organizations and their software vendors. SecureLink VSN is used by over 10,000 hospitals, banks, government agencies and others to replace modems and as an easy, secure and auditable alternative to desktop sharing and VPNs.

Your challenge: Enabling remote access for your software vendor's support technicians

Enterprise software applications are the backbone of business operations. Mission critical applications are complex and may require frequent support and service delivered from the software vendor's support center.

Traditionally, vendors dialed in with modems. Today, they're using a mix of modems, VPNs, desktop sharing and other ineffective, insecure and un-auditable methods. This burdens your IT staff, creates security vulnerabilities and challenges compliance with regulations. Service levels and uptime suffer.



The solution: SecureLink Virtual Support Network

SecureLink VSN was specifically designed to address the unique challenges of enabling remote access for software vendors in high security environments. You gain full control of all connection rules while easily enabling your software vendor to deliver the support and service to keep your enterprise software applications running.

Secure.

- True authentication
- Granular privilege control
- End-to-end encryption
- Access scheduling
- Much more

Simple.

- 5 minute basic installation
- No hardware
- Browser based
- Online training tutorial
- Free support

Auditable.

- High definition audit at the individual technician level
- E-mail connection notifications
- Real-time monitoring
- Fully exportable report data

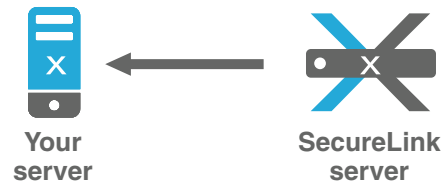
Secure, simple, auditable and used by more than 10,000 security conscious and highly regulated customers today.

How it works - SecureLink Virtual Support Network

Used today by over 10,000 security conscious and highly regulated customers, Enexity's SecureLink VSN provides secure and efficient remote network access for your software vendors.

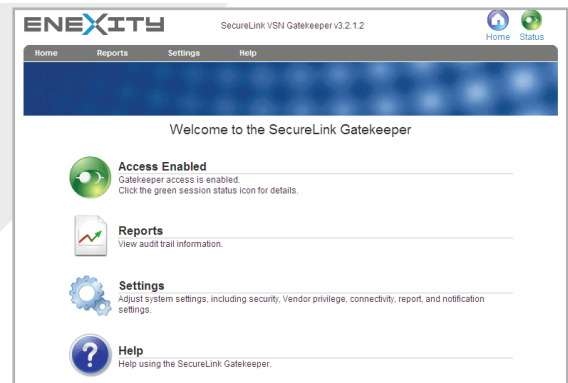
Step 1: Download SecureLink VSN Gatekeeper

The Gatekeeper is a lightweight software component that is installed one time to a single server. The Gatekeeper can be downloaded, installed and enabled in less than 5 minutes.



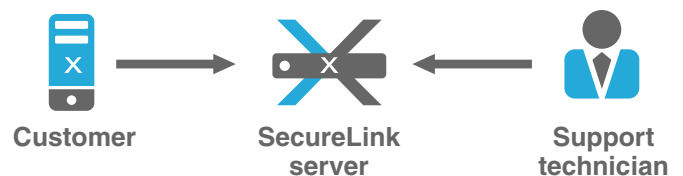
Step 2: (Optional) Configure Gatekeeper rules

If desired, you may modify the Gatekeeper's default settings, including when access is enabled, what privileges are granted to the support technicians and other options such as encryption strength and reporting.



Step 3: Connection made

The Gatekeeper makes an encrypted, outbound connection to the vendor's dedicated SecureLink Server. The support technician is authenticated, SecureLink enforces your rules while auditing all activity.



Technical specifications

Supported platforms	Windows, Linux, Solaris, AIX, OS400, HP-UX, Tru64, Mac OSX, VMWare, Java Applet and more
SecureLink VSN server	Operating system: RedHat Linux, Fully J2EE compliant Recommended hardware: Dell PowerEdge, hosting available in our data center
Encryption	Up to and including 256 bit AES, configurable by customer
Supported services	Any TCP-based service, including: SSH, telnet, RDP, desktop sharing, FTP, database, HTTP

Security overview – Why SecureLink VSN is more secure than a VPN for vendor network access

Individual accountability- With a VPN account, it's common for VPN credentials to be stored in the vendor's CRM system (or written on a sticky note) and shared among multiple technicians. SecureLink VSN requires individual accounts for each technician.

Remote authentication- The support technician login is authenticated remotely using the vendor's preferred authentication method, including Active Directory and LDAP. Maintaining a local list of logins and passwords for your vendors is challenging, if not impossible unless you receive a daily listing of new hires & terminations or staff a help desk to manually enable and disable accounts.

Granular permission control- Your vendor's technicians will only be able to access the services which you permit. Access rights are administered at the port level per machine. For example, you may only enable RDP to a single server, or may wish to enable multiple services, such as FTP, telnet, HTTP, databases on one or more servers.

Credential privacy- The SecureLink Gatekeeper can store network credentials (logins) for your network resources. The support technician may access these permitted network resources without ever seeing the login & password. This protection is clearly superior to having secure customer credentials stored in the vendor's CRM system or on sticky notes.

Encryption- SecureLink sessions are encrypted from end-to-end. You may select your preferred encryption, including 128 AES, 3DES, 256 and others.

Dedicated servers- Each SecureLink VSN Server is dedicated for a single vendor and is typically housed in the vendor's DMZ. This security feature is especially relevant in industries where policies or regulations prohibit the transfer of sensitive information.

Grouping- Support technicians may be grouped according to the customers they are permitted to support. This feature is especially valuable in government applications that require special security clearances, such as background checks or fingerprints on file.

Single session authorization- Access for the vendor can be manually initiated for a variable period of time. For example, you may wish to enable access for only the next 3 hours.

Access scheduling- The SecureLink Gatekeeper can be configured to enable access via a schedule, such as Monday – Friday from 8:30 AM to 5:00 PM and Saturdays from 9:00 AM to noon.

Connection notification- You can receive e-mail notifications each time a support technician connects. These notifications include details, such as the name of the technician and the server being accessed.

Monitoring- SecureLink VSN sessions can be monitored via a browser from anywhere within your network.

High definition audit trail- The Gatekeeper maintains a detailed audit of all activity at the individual user level, ensuring individual accountability and compliance with industry regulations. The audit includes services accessed, files viewed or transferred, commands entered and more.

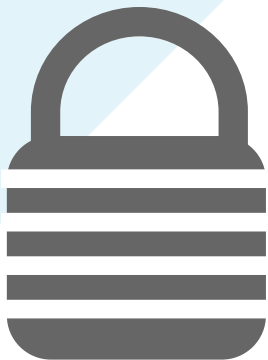
Audit export- The Gatekeeper audit trail can be easily exported to syslog or another central reporting repository.

“We would like all our software vendors to use SecureLink & we are going to encourage them to do so.”

- Jack Hennessy

Project Manager

Community General Hospital of Syracuse



SecureLink VSN Frequently Asked Questions

Q: What is the SecureLink VSN & how does it work?

A: SecureLink VSN is a Virtual Support Network solution made by Enexity. SecureLink VSN is specifically designed to help security conscious and highly regulated customers receive enterprise software support in a way that is simple, secure, and auditable.

Q: How does using SecureLink VSN benefit me?

A: SecureLink VSN helps you have issues resolved faster, without sacrificing security or compliance. Over 70% of the total cost of enterprise software ownership is the ongoing maintenance and support. SecureLink VSN helps you maximize the value of this investment in a very simple, secure, and auditable way.

Q: Who else is using SecureLink VSN?

A: SecureLink VSN is used today by more than 10,000 highly secure and heavily regulated organizations. SecureLink has been reviewed and accepted by organizations in healthcare, financial services, government, pharmaceutical, legal, gaming, manufacturing and other secure industries.

Q: Is SecureLink VSN secure?

A: SecureLink VSN was designed from the ground up to give you a superior level of security, control and audit. SecureLink VSN has features specifically necessary for the unique requirements of enabling 3rd party network access including: individual accounts for each support technician, remote authentication, a high definition audit trail of individual user activity, manually initiated sessions or access scheduling, real-time connection notifications delivered to your e-mail, granular permission controls and real-time monitoring.

Q: We enable access for our vendors with our VPN. How is SecureLink VSN similar to, or better than a VPN?

A: SecureLink VSN is similar to a VPN in that it enables remote network access. However, for enabling remote access for your software vendors and other 3rd parties, SecureLink VSN offers additional security, control and audit with less effort and infrastructure. With a VPN account, it's typical for more than one support technician (sometimes hundreds) to share a login, making accountability and compliance impossible. While you may issue individual VPN accounts and key fobs to each individual, but these burdensome policies don't typically last when the support technicians must provide a drivers license, social security number, etc. Additionally, unless the software company provides a daily list of employees who have been hired & fired, it's impossible to be certain if an account should still be active. SecureLink VSN authenticates the support technician with their own Active Directory (or LDAP) account, ensuring authentication and individual accountability. SecureLink VSN also offers unique features, such as access scheduling, connection notification delivered via e-mail, real-time monitoring and an audit trail that captures detailed activity (including files accessed, commands entered) at the individual technician level.

Q: We use WebEx to allow our vendors to support us, how does this compare to SecureLink?

A: Desktop sharing services, like WebEx or GoToMyPC, are excellent for supporting desktop applications and quite useful for training purposes. SecureLink VSN includes these desktop sharing capabilities, while simultaneously providing functionality required to support enterprise applications in high security environments. These include access to non-Windows environments, the ability to restrict access to individual ports on individual machines, access scheduling, remote authentication, connection notification, high-definition audit trails and much more.

Q: What do I need to install on my network?

A: You install and configure a SecureLink Gatekeeper, a small piece of software (+/- 10 MB) that can be downloaded from your vendor's SecureLink server in minutes. The Gatekeeper is accessible via a browser and fully configurable with a simple user interface.

Q: Where do I install the Gatekeeper?

A: The Gatekeeper is typically installed on one of your servers running the vendor's application. Depending on your use-case, the vendor may ask you to install more than one Gatekeeper, or a single Gatekeeper may be utilized to enable access to multiple servers. Native Gatekeepers are available for virtually any operating system.

Q: Does the Gatekeeper put a load on my server?

A: The Gatekeeper requires an absolute minimum of memory and processor while waiting for a connection, running as a background service requiring about 3K of memory.

Q: Who can have access to my Gatekeeper?

A: Only the support technicians with the appropriate credentials may access your network. At the vendor's support center, each technician must log into SecureLink VSN with an individual login and is authenticated using their preferred method, such as Active Directory or LDAP. Your software vendor may also have restricted access to your Gatekeeper to certain segments of their users. In certain government applications, for example, the vendor may restrict access to only those technicians with a fingerprint or FBI background check on file.

Q: When can they have access to my network?

A: Access can be enabled manually by you for a certain period of time (ex: turn on access for 2 hours or 2 days), can be scheduled for certain days and times (ex: Monday – Friday from 8:30 – 5:00 and Saturday from 9:00 – 12:00) or can be enabled for access any time.

Q: What can the support technician do once connected?

A: The Gatekeeper enables only the privileges you approve, which can be configured at the machine and port level. For example, you may want to enable access to RDP on a Windows server, telnet on a Unix server and an Oracle database port on the database server.

Q: How will I know when someone is accessing our network?

A: The Gatekeeper can be configured to e-mail connection notifications to one or more people. The connection notification will indicate who has connected, what server they're connected to and may also contain relevant information about the support ticket or issue being worked.

Q: How will I know what's been done?

A: The Gatekeeper maintains a detailed historical audit of all activity at the individual user level. This information is available in real-time and can also be exported to syslog or another local reporting repository.

Q: Is SecureLink compliant with HIPAA, GLB, PCI, FIPS, CJIS or other industry regulations?

A: Products themselves can't be compliant with any regulation. It's the proper implementation of a product like SecureLink VSN that achieves compliance. Each of the regulations listed above has unique language, but all of them have the same principles: protect the privacy and security of information with well defined procedures and a detailed audit trail. SecureLink VSN, properly utilized, fully meets the most stringent interpretation of each of these regulations, and more importantly, the purpose for which they were enacted.

Q: I have additional questions that we not addressed here. Who should I contact?

A: Your vendor using SecureLink VSN should be able to answer most of your questions, but you may also contact Enexity online at www.enexity.com or via the phone at 512-637-8700 or 866-ENEXITY.

Q: We have dozens of other software vendors that are not yet using SecureLink VSN. Do you have a version of SecureLink that I can use with all of my vendors?

A: Yes, there is an enterprise version of SecureLink VSN that enables you to easily manage all of your software vendors on a secure and effective platform. To find out more about SecureLink Enterprise VSN, please visit www.enexity.com.