

Introducing SecureLink

A remote support platform designed for third-party access

SecureLink is proud to partner with technology providers that are committed to delivering secure, compliant, and next-generation support to their enterprise customers.

SecureLink is a third-party access solution specifically designed to manage the remote support connections between technology providers and enterprise customers in highly secure, regulated environments.

SECURELINK EXPANDS SUPPORT AND ENHANCES SECURITY



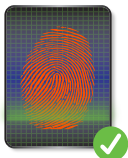
IDENTIFY

SecureLink provides advanced authentication methods that tie specific actions to the individual who performed them



CONTROL

Set the rules for access - Control when and how support reps connect, and receive notifications of all activity



AUDIT

Audit and record all activity with forensic level reports - Security and regulatory compliance is top priority

SecureLink Feature	Enterprise Customer Benefit
Strict Access Control	Restrict access to specific hosts and ports and keep your credentials private – Enable access manually or on a specific schedule.
Credential Storage	Network credentials are locally stored. Vendors don't require knowledge of usernames and passwords so your credentials can never be shared.
Individual Account Level Verification	No shared logins – Each support technician has a unique login with privileges assigned - this delivers strong access control and a granular session audit.
Email Notifications	No more ghosts on your system – With individual account authentication and email connection notifications, all access can be monitored and tracked in real time.
High Definition Audit and Reports Detailed Log Files Services Accessed Files Transferred	Accountability is clear – With simple and detailed reports, you can monitor who connected, when, to what systems, using what tools and for how long.

SecureLink is a powerful tool that allows your vendor to provide the very best in customer support.

Introducing the Gatekeeper

Why SecureLink?

Intuitive and Easy to use

Using SecureLink requires a simple one-time install of a small piece of software, called the Gatekeeper, on your vendor's application server. From there initiating a session requires only a web browser - you can complete the install in less than ten minutes.



Features:



Access Schedules



Credential Storage



Email Notifications



Built-in Screen Sharing Tool



Individual Account Level Audit

Powerful Control and Audit

SecureLink is different than VPN's, modems, and other solutions because it puts the customer in total control of vendor connectivity, while allowing technicians to resolve issues more efficiently.

- Allow access anytime, set up manual access windows, or even enable and disable access according to an access schedule.
- Receive a notification of whenever your vendor connects, as well as a full summary of access activity when a connection ends.
- Audit all vendor activity on your network.

Secure Access meets Efficient Support

SecureLink is like an on-demand VPN with next-generation security and audit. It allows your vendor access to powerful back-end resources, like RDP and SQL, while still enabling access to basic tools, like file transfer and desktop sharing.

Your vendor will have the connectivity needed to quickly resolve your issues. You'll have peace of mind knowing you have total control over remote access and a detailed report and video of all work performed.

High Definition Audit and Compliance

SecureLink provides a secure remote support solution to comply with the remote access standards of heavily regulated industries. Unlike many remote access tools, SecureLink boasts a best-in-class High Definition Audit feature that meets even the most complex requirements.

When you combine SecureLink's comprehensive authentication and access controls with an industry-leading audit, it's easy to verify compliance.

Addressed regulations include:

CJIS
FIPS 140-2
FIPS 197

FIPS 200
Gramm-Leach Bliley
HIPAA/HITECH

NIST SP-800
PCI DSS
Sarbanes-Oxley

Security Standards	SecureLink Functionality
Comprehensive Documentation	Detailed account of every support session includes: • Name of the person accessing the system • Reason for remote access • Description of work to be performed • Time stamps; start & end time of end-user remote access sessions • Hosts and Services used • RDP, TelNet and SSH audit
Audit and Reporting	On-demand reports to analyze all behavior and efficiently investigate abnormal activity: • Detailed log files • Services accessed • Files transferred • Time stamps; start/end time of remote access sessions
Transparency and Accountability	Clearly define responsibility: • Individual account level audit, users have unique activity fingerprints • Authorization, real-time monitoring, and control of all remote access for remote maintenance and diagnostic activity • Complete historical reporting

Gatekeeper FAQ

The SecureLink Gatekeeper is a software component designed to be installed on a single Windows or Unix Server. Its purpose is to serve as a secure access point into one or more servers on your network by trusted 3rd parties.

What are the technical requirements for a Gatekeeper?

- 512MB RAM
- 200MB Disk Space
- Outbound Internet Connection (DSL - 128 KB/s minimum)
- Outbound firewall access on Ports 22 and 80 to the SecureLink server

Will I have to make any changes to the Firewall?

The Gatekeeper requires internet access to communicate with your vendors SecureLink server, but there are no firewall changes necessary to enable your vendor to connect using SecureLink. If the Gatekeeper is installed on a system that does not have internet access, rules should be set on the firewall to allow SSH and HTTP access outbound directly to your vendor's SecureLink server.

Does the Gatekeeper require a dedicated workstation/server?

The Gatekeeper does not need a dedicated workstation/server.

Is a reboot required during installation?

The Gatekeeper installation does not include a server reboot.

How do I access my Gatekeeper?

To access your Gatekeeper you will navigate to your vendor's SecureLink server and log-in with your provided credentials. These credentials will automatically be emailed to you when your vendor creates your Gatekeeper account. You will need to request an account if you do not have one.

Local access to the Gatekeeper is also available and provides only limited administrative functionality. The Gatekeeper can be accessed locally in two different ways. From your Windows start menu, select **All Programs/SecureLink/SecureLink Gatekeeper**. You can also access the Gatekeeper from your browser by typing <http://127.0.0.1:4680> in the address bar.

How do I enable access for my vendor?

When installed, the Gatekeeper defaults to a state of Disabled. To enable, log in to your vendor's SecureLink server as a Gatekeeper admin using your provided credentials. Click on the Connection Status link. From there, you can enable access indefinitely or provide an access window after which the Gatekeeper will return to a disabled state.

To learn more about SecureLink and the Gatekeeper, please contact your vendor account manager or call 1-(SEC)-URE-LINK (732-873-5465).