opentext™

Product overview

OpenText SOCKS Client

Safe and secure access across firewalls for consumers, enterprises and OEMs

Offers protocol support

Includes platform support

Provides flexible IP access rules

Firewalls can impose severe restrictions on IP data traffic, leading to problems for software not using mainstream IP ports, such as mail and remote access protocols. Organizations require a solution that keeps firewalls effective and secure, yet still allow IP access to services behind the firewall.

OpenText™ SOCKS Client is a robust, Microsoft® Windows®-based SOCKS solution that allows users to access hosts securely on the other side of a firewall. SOCKS Client supports 32- and 64-bit Windows operating systems and is backed by a reliable, commercial-grade support organization.

The SOCKS protocol is designed to isolate corporate networks from outside attack, routing all connections from internal PCs to external services (e.g., HTTPS web servers and application servers) through a secure SOCKS proxy. SOCKS Client supports any SOCKS v4 or v5 compatible proxy, including those offered by Blue Coat, Cisco® and others. The SOCKS protocol operates at the transport layer, providing fast and secure forwarding of network traffic through firewalls, without impacting end user experience, with remote services and applications. Traffic forwarding rules are simple and flexible, supporting the "SOCKSification" of traffic based on the IP address or IP range of the remote system, or by selecting executables on the client machine to "SOCKSify."

Offers protocol support

Works with any SOCKS v4 or v5 compliant proxy solution and includes HTTP client authentication for proxy hosts, such as Blue Coat ProxySG. SOCKS Client fully supports IP v4 and v6 addressing.

Includes platform support

Install SOCKS Client on any supported version of Windows, including Windows 7, 8.1 and 10, as well as Microsoft® Windows® Server 2008 R2, 2012, 2016 and 2019.

opentext™

Download the trial

Keep up to date

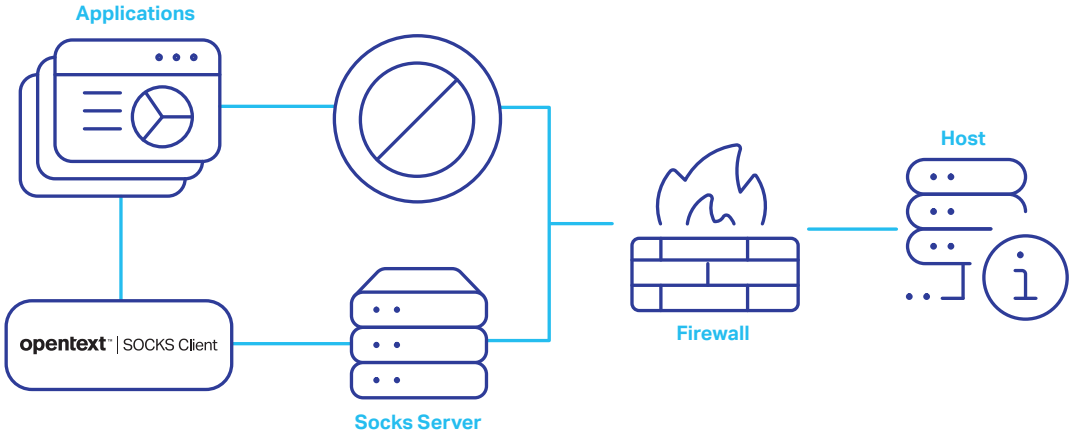
Learn more

Provides flexible IP access rules

Enable SOCKS forwarding based on the hostname, IP address or IP address range of the outside service. Users also have the option of enabling SOCKS forwarding for specific applications that require access services on the other side of the firewall.

SOCKS Client can be a part of a single sign-on initiative by allowing users to seamlessly authenticate SOCKS connections using Microsoft® Active Directory® or other Kerberos clients, such as OpenText Kerberos or MIT Kerberos.

To evenly distribute the load on SOCKS servers and provide greater reliability, SOCKS Client can randomly connect to SOCKS servers listed during configuration and provide load balancing and protection against any single point of failure. SOCKS Client is ready for centralized deployment with the support of the de facto Windows® Installer framework. An organization's decision to choose SOCKS Client is backed by a dependable, commercial-grade customer support organization that is second to none.



OpenText SOCKS Client allows firewalls to be crossed through a single point of entry, maintaining network infastructure integrity

Feature	Description
Connections operating systems	SOCKS v4 and v5
Network traffic	TCP, UDP*
Authentication*	Username/password combination, OpenText Kerberos, MIT Kerberos and Microsoft Kerberos (Active Directory)
Encryption*	Encrypt network traffic using industry standard GSSAPI, authentication only, integrity and confidentiality
DNS resolution*	Local, remote or local then remote
Platforms supported	Windows 10*, Windows 8.1*, Windows 7, Windows Server 2016 R2*, Windows Server 2012 R2*, Windows Server 2008 R2

*Windows Filtering Platform (WFP) applications are not supported

opentext.com/contact Twitter | LinkedIn