globalscape
securely connected

Data Sheet

scConnect

Key Features:

- Access your work desktop while you work remotely—from any device
- Share your files with other authorized users
- Administrators retain full control over who can access which files
- Complete audit trail, ensuring compliance with industry, government, and regulatory standards
- Integrates with Active Directory and multifactor authentication servers
- Enterprise Mobility Management (EMM) concerns dictate mobile policy

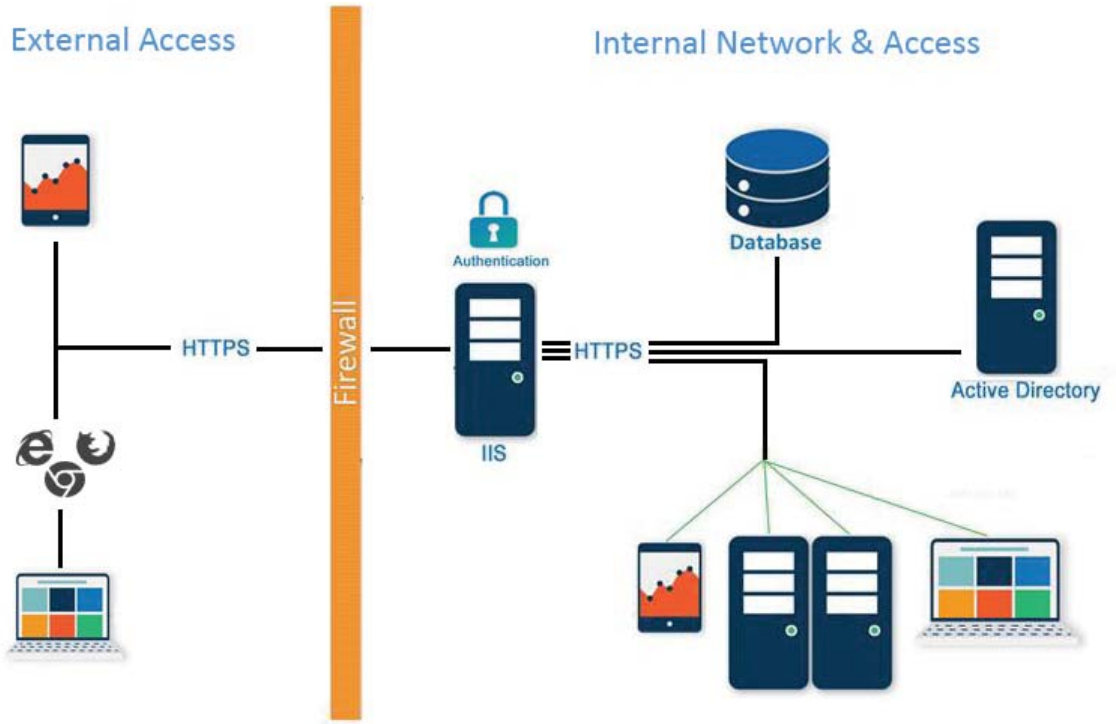
Share files securely—no matter where they are stored

Enterprise-Grade File-Sharing Solution

These days, your digital content can be stored on your desktop computer, work laptop, and servers—pretty much everywhere. However, that content can be tough to find, difficult to access, and impossible to share with colleagues when you are away from the office. scConnect™ is an enterprise-grade file sharing and access solution that offers consumer-grade usability, but with the security controls that IT demands, including on-premises configuration and management.

Secure, on-premises, centralized access and authentication

Provide employees with a secure option for file sharing without losing control of your network. On-premises deployment provides the mobile access (BYOD) you want with the local administration and security you require—your own private cloud without the dangers of cloud-sharing providers. Centralized administration for IT governance, two-factor authentication, and complete audit trails ensure compliance with industry, government, and regulatory standards. Doctors can allow patients to log in to see medical information, universities can make transcripts available, and contractors can access sensitive design documents, all while maintaining the security of your private network.



4500 Lockhill-Selma Road, Suite 150; San Antonio TX 78249; 1-800-290-5054 (USA & Canada); 1-210-308-8267 (Worldwide)

Allow Access While Retaining Security

scConnect Govern, the administration interface installed within the company's trusted network, is used to specify which users and which devices can access files, as well as the level of access they are allowed. Active Directory users and groups are imported from Active Directory to make setup easier. The administrator can enable and disable a user's ability to add devices, add links, and access externally, and can add/remove users from a shared file.

How Do Employees Access and Share Files?

Employees or administrators can install the scConnect service on their devices, such as company desktop and laptop computers, and select any files or folders they want to access remotely. Using scConnect's web interface, users can then specify folders and files they want to share and with whom to share them. The employee and anyone they've shared with can access the files from any browser or a mobile device as long as the device is turned on and running the scConnect service.

Users can access their data from anywhere in the world using mobile devices or any major web browser, enabling them to dissolve the barriers that prevent them from working and collaborating effectively.

Contact Us Today

Contact a solution specialist or visit our website for more information about scConnect™.

System Requirements

- **Administration interface:**
  - Microsoft Windows Server 2012 R2 or later
  - A least 1GB available RAM
  - Active Directory
  - SQL Server database
  - Microsoft IIS v8 (built in to Microsoft Windows Server 2012 R2)
  - Microsoft .NET v4 or later
- **Mobile devices:**
  - iOS or Android
- **Browsers:**
  - Chrome: Latest public release version (40 on release date)
  - Firefox: Latest public release version (35 on release date)
  - Internet Explorer: 11 and above

4500 Lockhill-Selma Road, Suite 150; San Antonio TX 78249; 1-800-290-5054 (USA & Canada); 1-210-308-8267 (Worldwide)