Version:	3.2	Date:	7/12/2013
Status:	**APPROVED FOR USE**		

Purpose

This document describes the Internet host names, services, and TCP ports required to use the ShotSpotter Flex client software. This document identified the host access, service, and port access required to use the Release 2013.1 versions of:

- ShotSpotter Flex Alerts Console
- ShotSpotter Flex Investigator Portal
- ShotSpotter Briefing Room (coming soon)
- ShotSpotter Siren (coming soon)

Future releases may change these requirements, at which point this document will be updated. A web-based tool called the SST System Profiler, can provide an automated assessment of whether a particular computer has the necessary proxy and content type access. See the *Verifying Access Using System Profiler* section below.

Required Access

To permit the collection of incident information for display, ShotSpotter Flex client software must be able to access services and specific data using network references outside the customer's network. Traffic is primarily HTTPS and is customarily provided via with an internal proxy server that also provides security from external intrusions and allows access to information and services that are within the access policies of the organization.

The ShotSpotter Alerts Console and Investigator Portal run within a Silverlight executable and reference ShotSpotter software services for access to customer specific data, incident notifications, historical incident lists. The ShotSpotter Briefing Room is an *in*-browser Silverlight application requiring similar access. ShotSpotter Siren requires only port 80 and 443 access. Here is a complete list of required access to host names, services, and TCP ports:

Host Name	Purpose	Service(s)	TCP Port(s)
us1.shotspotter.net **us2.**shotspotter.net **us3.**shotspotter.net **us4.**shotspotter.net **us5.**shotspotter.net	ShotSpotter Flex datacenter. These servers act as the primary application servers.	HTTPS	443
***.shotspotter.net**	Additional wildcard access for *.shotspotter.net will permit Siren and Briefing Room access (coming soon). For Siren, a single FQDN (e.g., ABCpolicedept.shotspotter.net) will actually be used.	HTTP HTTPS	80 443
host15.4txlacc.net	ShotSpotter Flex datacenters (different physical location), domain name 2 of 2. These servers act as the primary application servers.	HTTPS	443
chat.shotspotter.com	Encrypted incident chat between users and SST, Inc. review center, 24x7x365. System profiler functionality to confirm required network access.	HTTPS	443
auth.shotspotter.com or auth.shotspotter**.net**	User authentication and login (redirect)	HTTP HTTPS	80 443
dev.virtualearth.net **ecn.t0**.tiles.virtualearth.net **ecn.t1**.tiles.virtualearth.net **ecn.t2**.tiles.virtualearth.net **ecn.t3**.tiles.virtualearth.net **ecn.t***.tiles.virtualearth.net	API authentication and redirect Map tiles (Microsoft) (Microsoft-recommended wildcard rule)	HTTP HTTP HTTPS	80 80 443
verisign.com **usertrust.com** **netsolssl.com**	SSL Certificate root authorities sometimes required if workstation has an out-of-date list of authorized root certificates.	HTTP HTTPS	80 443

Technical Description of Network Activities

In addition to application data, file are retrieved from the Virtual Earth sites and the ShotSpotter servers in benign compressed media file formats (`.jpg`, `.png`, and `.mp3`) which are interpreted by the ShotSpotter application in the most restricted execution environment within Silverlight. File system access to cache the retrieved data and log the user's activity is done within Isolated Storage provided by the Silverlight virtual file system and limited to a maximum total size with a default of 25MB. If a user clicks the "Copy to Clipboard" in order to copy incident details to the clipboard button (for pasting into a CAD or RMS system, for example) in the ShotSpotter Flex Alert Console, the application are done through the Silverlight Safe-Critical Code method that, when requested by user interaction, validates both user initiation and the information to be passed.

The network traffic generated by ShotSpotter Flex applications varies according to the number of incidents processed and previously cached items. On initial startup, applications gather general information regarding the customer's coverage area and recent activity so that users can browse, search for, and display historical incident records. When handling a gunshot incident, location specific mapping and audio information is retrieved by the client.

With the exception of publicly-available map tiles provided by Microsoft, certain API access steps, and help files, all traffic is encrypted using Transport Layer Security (TLS, the successor to Secure Socket Layer, SSL). The IP addresses of `*.virtualearth.net`, e.g. `dev.virtualearth.net 65.55.84.143`, is authoritatively supplied by `glb1.glbdns.microsoft.com` and `glb2.glbdns.microsoft.com` and the domain is registered by CSC Corporate Domains. SST, Inc. servers present valid SSL certificates provided by Network Solutions, Inc., which confirm the IP addresses of each server.

The following table summarizes the network traffic including protocol overhead under various conditions.

Alert Console

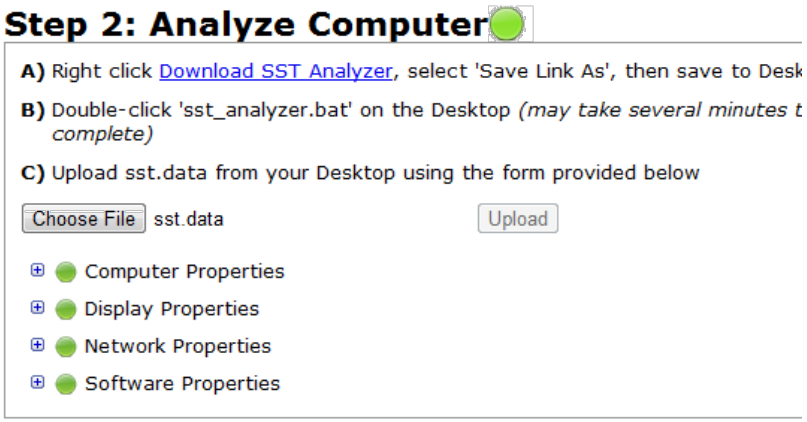
Action	Estimated Data Transfer
Installation/Upgrade (download local web app)	2.4mb
Launch + login (no tiles cached)	750kb
Launch + login (tiles cached)	25kb
New Incident (no tiles cached)	950kb
Incident Refresh (tiles cached)	13kb
Zoom In, Road Map (no cache)	980kb
Switch to Birds-Eye View (no cache)	870kb
Audio Clip (Mobile/Patrol only), per clip	20kb

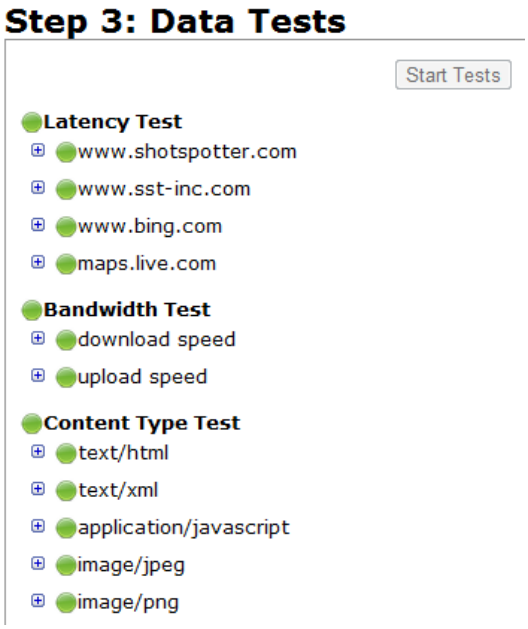
Investigator Portal

Action	Estimated Data Transfer (kb)
Installation/Upgrade (download local web app)	2mb
Launch + login (no tiles cached)	200kb
New Incident (no tiles cached)	950 kb
Audio Clip, per clip	20kb

Verifying Access Using Compatibility Checker

SST has developed a web-based tool to aid in verifying system configuration and network access required for using the ShotSpotter Flex clients. The client can be accessed at http://chat.shotspotter.com/profiler. Customers or customers' IT representatives may use this tool *at each computer* which will access the ShotSpotter Flex service.





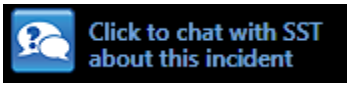
The Profiler lists basic system configuration and verifies access to all of the above host names and services. In addition to tests run from within the web-browser, users will download and execute a small batch (.bat) file, the contents of which are available for inspection before use. Users may also review the data collected by this batch file before it is uploaded to SST for debugging and support purposes.

Support

SST Customer Support is available to all customers with valid ShotSpotter Flex Support contracts. You may contact SST Customer Support:

Via Live Chat:

From either the ShotSpotter Flex Alert Console or the ShotSpotter Flex Incident & Reports Portal, look for the chat links:



or by following this link in any web browser:

https://chat.shotspotter.com/chatrequest

Via Phone:

Phone support is available Monday-Friday, 8:00 am to 5:00 pm Pacific Standard Time. Please contact our support team during these hours at: +1 (888) 274–6877, then dial option 4.

Via Email:

Email support@shotspotter.com. Please include as much detail as possible so we may better serve you quickly.