FED-72-03

IT Administrator Tips - Group Policy Application Permissions for ShotSpotter Flex Alerts Console and Incident and Reports Portal

Version:	1.1	Date:	2/1/2013 8:05:00 AM
Status:	**Approved for Use**		

Purpose

This document describes the restricted privileges execution environment in which ShotSpotter Flex applications run and how administrators can enforce security. ShotSpotter Flex applications operate entirely within the fully-secure Silverlight security-restricted execution environment. The general system requirements for ShotSpotter Flex are available on the SST website[i]. In additional, documents detailing network access and endpoints required[ii] to support ShotSpotter Flex and an installation guide are also available from SST customer support.

Background

Both ShotSpotter Flex applications (the Alert Console and the Incident & Reports Portal) operate as out-of-browser (OOB) Microsoft Silverlight applications. (There is no ShotSpotter Flex executable. All Silverlight OOB applications run within the `sllauncher.exe` process, which is essentially a special version of Internet Explorer designed solely to host Silverlight applications.) There are two types of Microsoft Silverlight OOB applications: *sandboxed*, which are severely restricted; and *elevated trust*, which are permitted to access data from multiple SSL sources, interact with the clipboard, save files locally, and perform other similar functions. In order to provide necessary functionality (access to ShotSpotter data on cloud-based servers, export incident data to file, copy/paste, etc.) our Flex applications run under elevated trust. For details, please review the Microsoft Silverlight Security Overview[iii] for Silverlight.

No Administrator Required

In a normal Windows domain environment, installation of elevated trust applications *does not require system administrator or power user privileges* for the local (or domain) Windows user. Any user, including the Guest user account, can install the ShotSpotter Flex applications—either the Alert Console or the Incident & Reports Portal. Most system administrators do not restrict their users from installing such applications.

Restricting Installations After Flex

There are two domain-level Group Policy Settings which control the execution and use of Silverlight OOB trusted applications within your domain. By default, these settings permit users without administrative rights to install and use Silverlight OOB applications. These group policy settings are detailed in this Microsoft Silverlight Group Policy Settings resource guide[iv]. You may apply these using the Group Policy tools[v] or using the new ADMX file[vi] techniques.

After the ShotSpotter Flex OOB applications have been installed, you may choose to *turn off* the group policy permitting the installation of *new* OOB applications. This will not negatively affect already-installed applications, which will continue to run.

Please note that there is also a Group Policy Setting which permits you to control whether users can launch any trusted applications at all. *Do not enable this policy* because it will disable all Silverlight OOB applications requiring elevated trust, *including ShotSpotter Flex*.

For your convenience, we have duplicated the pertinent settings here:

Domain Policy: Prohibit Installation of New Trusted Silverlight Applications

Caution: You must enable this policy to install ShotSpotter Flex Alert Console and Incident & Reports Portal. Although most administrators choose not to do so, you may subsequently disable this policy once installation is complete.

Key Path	HKEY_LOCAL_MACHINE\Software\Microsoft\Silverlight\
Value Name	AllowLaunchOfElevatedTrustApps
Value Type	DWORD
Valid Values	Disabled: 0x00000000 Enabled: 0x00000001

Domain Policy: Prohibit Launch of Any Trusted Silverlight Applications

Warning: Enabling this policy will disable the ShotSpotter Flex applications and any other Silverlight OOB application. This setting is not compatible with ShotSpotter Flex or any other Silverlight OOB trusted application. Make sure you disable this policy if you wish to use ShotSpotter Flex.

Key Path	HKEY_LOCAL_MACHINE\Software\Microsoft\Silverlight\
Value Name	AllowInstallOfElevatedTrustApps
Value Type	DWORD
Valid Values	Disabled: 0x00000000 Enabled: 0x00000001 ← Warning: do not use!

Links and References

[i] "ShotSpotter Flex System Requirements" http://www.shotspotter.com/technology/system-requirements. Also available as PDF from SST customer support: *FED-72-02 System Requirements for ShotSpotter Flex.*

[ii] Available as PDF from SST customer support *FED-72-01: Hosts and Services Required to Use ShotSpotter Flex Clients*.

[iii] *Silverlight Security Overview* http://download.microsoft.com/download/A/1/A/A1A80A28-907C-4C6A-8036-782E3792A408/Silverlight%20Security%20Overview.docx

[iv] "Group Policy Settings" http://www.microsoft.com/getsilverlight/resources/documentation/grouppolicysettings.aspx

[v] "Deploying Custom Registry Changes through Group Policy" http://blogs.technet.com/b/askds/archive/2007/08/14/deploying-custom-registry-changes-through-group-policy.aspx

[vi] http://technet.microsoft.com/en-us/library/cc709647(v=ws.10).aspx