# EFT OpenSSL Registry Overrides

## Introduction

With the exception of the SFTP (SSH2) protocol, all EFT inbound and outbound connections (beginning with EFT version 7.1.1) now use the global SSL settings to determine which OpenSSL cipher suites and protocol versions are exposed/used. There may be instances where customers require more fine-grained control over SSL settings. To address this, EFT now recognizes a number of registry entries that may be used to override the global SSL settings.

## Base Registry Path

All registry overrides are located under the following base path within the registry:

**HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\GlobalSCAPE Inc.\EFT Server 4.0\Config\SSL**

This includes both client-side (Admin User Interface and COM API client) and server side (EFT inbound and outbound) overrides. Note: Throughout this document the string **[Base Path]** is used as shorthand for the full base path outlined above.

## Override Levels

An override level refers to a specific registry key (path) that contains SSL overrides that apply to that level. Regardless of the level of the override, the same registry entries may be specified. For example, the registry override level that applies to all outbound connections at the global (server) level is **OutboundConnection**. Registry entries that are intended to apply to all outbound connections would therefore be placed under the following registry path:

**HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\GlobalSCAPE Inc.\EFT Server 4.0\Config\SSL\OutboundConnection**

Some overrides may be specified at the individual Site level. These exist as keys that reside under the path (within the aforementioned base path) **SiteLevel\[Site name]** where [Site name] is the actual name of the Site the override(s) apply to. For example, to specify overrides for all outbound connections for a Site named “MySite” you would place override entries under the following registry path:

**HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\GlobalSCAPE Inc.\EFT Server 4.0\Config\SSL\SiteLevel\MySite**

Finally, overrides may be applied to an individual Event Rule. These may be specified at the global (server) level or Site level. At the global level, overrides are placed under **EventRule\[Event Rule Name]** where [Event Rule Name] is the actual name of the Event Rule the overrides apply to. Event Rule overrides specified at the global level apply to all Event Rules with the specified name, regardless of what Site they belong to. In other words, overrides at this level apply across all Sites.

At the Site level, overrides are placed under the **SiteLevel\[Site name]\EventRule\[Event Rule Name]** where [Site name] and [Event Rule Name] are the actual names of the Site and Event Rule the overrides apply to respectively. Note that Site level overrides take priority over global ones.

## Available Override Entries

At each override level (i.e. server level, Site level, Event Rule level, etc.) you may specify the SSL Protocol version(s) and/or list of ciphers to be used. Both entries are optional and entries that exist but are empty (blank) are ignored. The available entries are available:

| Entry Name | Format | Description |
|---|---|---|
| **CipherList** | REG_SZ (String) | Specifies the list of ciphers to be used. |
| **ProtocolVersions** | REG_SZ (String) | Specifies the list of allowed OpenSSL protocol versions (i.e. SSLv2, TLS 1.0, etc.). |

The **CipherList** entry specifies a list of ciphers and follows the same syntax as that of the "manual" string field provided in EFT's Administration User Interface (located within the Security tab at the host level). Specially, the list may contain one or more ciphers delimited (separated) by colons. Also, there are a number of pre-defined identifiers available that refer to a set of cipher suites. For example, to include all cipher suites that employ the AES cipher you can simply include "AES" in the cipher list rather than list all the individual AES cipher suites. For a complete list of available identifiers as well as a comprehensive description of the cipher list format, please refer to the following webSite:

https://www.openssl.org/docs/apps/ciphers.html

Please note that the cipher list itself is case-sensitive. This is because the cipher list is passed to the OpenSSL library, which evaluates the cipher list in a case-sensitive manner.

The **ProtocolVersions** entry specifies a list of one or more SSL protocol versions to expose/enable separated by colons. Additionally, the list may contain the string "All" in the list to refer to all available protocol versions. Including an entry in the list indicates that the specified version should be enabled. Including "All" in the list indicates that all available protocol versions should be enabled. Protocol versions you do not wish to enable may simply be omitted from the list or explicitly disabled by preceding the protocol version with an exclamation point (logical operator) or a minus sign. For example, if you wanted to include all available protocol versions *except* SSL versions 2 and 3 (which contain known weaknesses/vulnerabilities) you could specify:

**All:!sslv2:!sslv3** or **All:-sslv2:-sslv3**

Note that unlike cipher selection string used with the **CipherList** registry override entry, strings specified with the **ProtocolVersions** registry override and not case sensitive. In addition, here are a few additional notes regarding the list of protocols specified using the **ProtocolVersions** override entry:

- A blank list is simply ignored.

- The list is evaluated strictly from left to right, and, by default, all protocols are disabled.
- Lists that equate to no protocols (i.e. tlsv1.1:tlsv1.2:!ALL) are ignored and are logged as an ERROR to EFT's log file.
- The available protocol version strings currently consist of "SSLv2", "SSLv3", "TLSv1", "TLSv1.1", "TLSv1.2" as well as "ALL". Additional version strings will be added in the future as new protocol versions are added to OpenSSL. EFT's COM API can be used to query the list of available protocol strings (using the ICIServer object's AvailableSSLVersions property).

## Administrative UI and COM API Overrides

When connecting to a remote EFT server (and the "Require SSL for remote administration" option is enabled on the server) overrides may exist that specify the SSL options used by the Administrative User Interface and the COM API. Note that these overrides need to be specified on the machine the Admin UI and/or COM API are being run from. The available override levels (keys) are supported:

| Override key | Description |
|---|---|
| **[Base Path]\AdminClient** | Overrides under this key specify the SSL options to be used by the Administrative UI client when connecting to an EFT server. |
| **[Base Path[\COMClient** | Overrides under this key specify the SSL options to be used by the COM API when connecting to an EFT server. |

Inbound Admin connections (from both the Admin UI and COM API) to the EFT server may use different SSL settings by placing override entries under the **AdminServer** override key. Note that these entries must be specified in the registry of the machine the EFT server is running on. Also, as with the client-side Admin UI/COM API overrides, the **AdminServer** overrides only apply if the "Require SSL for remote administration" option is enabled on the server side.

# Overrides for Inbound Client Connections to EFT

Overrides that affect inbound EFT connections are available at both the global (server) level and Site level. The following table summarizes the available global overrides:

| Override key | Description |
|---|---|
| **[Base Path]\InboundConnection** | Overrides under this key specify the SSL options to be used for all inbound client connections with the exception of the SFTP protocol |
| **[Base Path]\InboundConnection\HTTPS** | Overrides under this key specify the SSL options to be used for all inbound client connections using the HTTPS protocol. Note that this override has priority over the InboundConnection override. |
| **[Base Path]\InboundConnection\FTPSExplicit** | Overrides under this key specify the SSL options to be used for all inbound client connections using the FTPS (Explicit mode) protocol. Note that this override has priority over the InboundConnection override. |
| **[Base Path]\InboundConnection\FTPSImplicit** | Overrides under this key specify the SSL options to be used for all inbound client connections using the FTPS (Implicit mode) protocol. Note that this override has priority over the InboundConnection override. |

Site level overrides have priority over global level overrides. That is, EFT will use a Site-level override (if present) before it will use a global one. The table below summarizes the available Site-level overrides that affect inbound client connections. Note that the string <Site> is used as a placeholder for the name of the Site the override applies to.

| Override Key | Description |
|---|---|
| **[Base Path]\SiteLevel\<Site>\InboundConnection** | Overrides SSL options used for all inbound connections to Site <Site> with the exception of the SFTP protocol. |
| **[Base Path]\SiteLevel\<Site>\InboundConnection\HTTPS** | Overrides SSL options used for inbound client connections using the HTTPS protocol to Site <Site>. |
| **[Base Path]\SiteLevel\<Site>\InboundConnection\FTPSExplicit** | Overrides SSL options used for inbound client connections using the FTPS (Explicit mode) protocol to Site <Site>. |
| **[Base Path]\SiteLevel\<Site>\InboundConnection\FTPSImplicit** | Overrides SSL options used for inbound client connections using the FTPS (Implicit mode) protocol to Site <Site>. |

# Overrides for Outbound Client Connections from EFT

Overrides that affect outbound EFT connections are available at both the global (server) level and Site level and can be specified by protocol used, Event Rule action (i.e. copy, move, download, and AS2 send), and finally for a specific Event Rule. Below are the available overrides available at the global level. Note that the string <Event Rule>is used as a as placeholder for the name of the event the override applies to.

| Override Key | Description |
|---|---|
| **[Base Path]\OutboundConnection** | Overrides SSL options for all outbound connections with the exception of the SFTP protocol. |
| **[Base Path]\OutboundConnection\HTTPS** | Overrides SSL options for all outbound connections using the HTTPS protocol. |
| **[Base Path]\OutboundConnection\FTPSExplicit** | Overrides SSL options for all outbound connections using the FTPS (Explicit mode) protocol. |
| **[Base Path]\OutboundConnection\FTPSImplicit** | Overrides SSL options for all outbound connections using the FTPS (Implicit mode) protocol. |
| **[Base Path]\CopyAction** | Overrides SSL options for all outbound connections associated with Event Rule copy actions. |
| **[Base Path]\MoveAction** | Overrides SSL options for all outbound connections associated with Event Rule move actions. |
| **[Base Path]\DownloadAction** | Overrides SSL options for all outbound connections associated with Event Rule download actions. |
| **[Base Path]\AS2SendAction** | Overrides SSL options for all outbound connections associated with Event Rule AS2 send actions. |
| **[Base Path]\EventRule\<Event Rule>** | Overrides SSL options for outbound connections associated with Event Rule <Event Rule> |

As with the global overrides that pertain to outbound connections, Site level connections may be specified by protocol used, Event Rule action, and for a specific Event Rule. The table below summarizes the available overrides for outbound connections that exist at the Site level. Note that the strings <Site> and <Event Rule> are placeholders for Site name and Event Rule name respectively.

| Override Key | Description |
|---|---|
| **[Base Path]\SiteLevel\<Site>\OutboundConnection** | Overrides SSL options for all outbound connections associated with <Site> with the exception of the SFTP protocol. |
| **[Base Path]\SiteLevel\<Site>\OutboundConnection\HTTPS** | Overrides SSL options for all outbound HTTPS connections associated with <Site>. |
| **[Base Path]\SiteLevel\<Site>\OutboundConnection\FTPSExplicit** | Overrides SSL options for all outbound FTPS (Explicit mode) connections associated with <Site>. |
| **[Base Path]\SiteLevel\<Site>\OutboundConnection\FTPSImplicit** | Overrides SSL options for all outbound FTPS (Implicit mode) connections associated with <Site>. |
| **[Base Path]\SiteLevel\<Site>\CopyAction** | Overrides SSL options for all outbound connections associated with Event Rule copy actions for <Site>. |

| Override Key | Description |
|---|---|
| **[Base Path]\SiteLevel\<Site>\MoveAction** | Overrides SSL options for all outbound connections associated with Event Rule move actions for <Site>. |
| **[Base Path]\SiteLevel\<Site>\DownloadAction** | Overrides SSL options for all outbound connections associated with Event Rule download actions for <Site>. |
| **[Base Path]\SiteLevel\<Site>\AS2SendAction** | Overrides SSL options for all outbound connections associated with Event Rule AS2 send actions for <Site>. |
| **[Base Path]\SiteLevel\<Site>\EventRule\<Event Rule>** | Overrides SSL options for all outbound connections associated with Event Rule <Event Rule> for Site <Site>. |

## Evaluation order for outbound connection Overrides

When multiple overrides exist (at the global and/or Site levels) overrides are evaluated in a specific sequence with some overrides having precedence over others. Here is the exact order the overrides are evaluated in with the highest-priority ones being checked first.

1. [Base Path]\SiteLevel\<Site>\EventRule\<Event Rule>
2. [Base Path]\SiteLevel\<Site>\<action> where <action> = DownloadAction, MoveAction, CopyAction, or AS2SendAction depending on the Event Rule action being performed.
3. [Base Path]\SiteLevel\<Site>\OutboundConnection\<protocol> where <protocol> is HTTPS, FTPSExplicit, or FTPSImplicit, depending on the protocol being used.
4. [Base Path]\SiteLevel\<Site>\OutboundConnection
5. [Base Path]\EventRule]\>Event Rule>
6. [Base Path]\<action> where <action> = DownloadAction, MoveAction, CopyAction, or AS2SendAction depending on the Event Rule action being performed.
7. [Base Path]\OutboundConnection\<protocol> where <protocol> is HTTPS, FTPSExplicit, or FTPSImplicit, depending on the protocol being used.
8. [Base Path]\OutboundConnection