Compatibility

All PCs are compatible. But some of them are more compatible than others.
Unknown

Here we talk about backward compatibility to other SSL solutions. As you perhaps know, mod_ssl is not the only existing SSL solution for Apache. Actually there are four additional major products available on the market: Ben Laurie's freely available Apache-SSL (from where mod_ssl were originally derived in 1998), RedHat's commercial Secure Web Server (which is based on mod_ssl), Covalent's commercial Raven SSL Module (also based on mod_ssl) and finally C2Net's commercial product Stronghold (based on a different evolution branch named Sioux up to Stronghold 2.x and based on mod_ssl since Stronghold 3.x).

Table Of Contents

The idea in mod_ssl is mainly the following: because mod_ssl provides mostly a superset of the functionality of all other solutions we can easily provide backward compatibility for most of the cases. Actually there are three compatibility areas we currently address: configuration directives, environment variables and custom log functions.

Configuration Directives

For backward compatibility to the configuration directives of other SSL solutions we do an on-the-fly mapping: directives which have a direct counterpart in mod_ssl are mapped silently while other directives lead to a warning message in the logfiles. The currently implemented directive mapping is listed in Table 1. Currently full backward compatibilty is provided only for Apache-SSL 1.x and mod_ssl 2.0.x. Compatibility to Sioux 1.x and Stronghold 2.x is only partial because of special functionality in these interfaces which mod_ssl (still) doesn't provide.

Old Directive	mod_ssl Directive	Comment
Apache-SSL 1.x & mod_ssl 2.0.x compatibility:		
`SSLEnable`	`SSLEngine on`	compactified
`SSLDisable`	`SSLEngine off`	compactified
`SSLLogFile` *file*	`SSLLog` *file*	compactified
`SSLRequiredCiphers` *spec*	`SSLCipherSuite` *spec*	renamed
`SSLRequireCipher` *c1* ...	`SSLRequire %{SSL_CIPHER} in {"`*c1*`", ...}`	generalized
`SSLBanCipher` *c1* ...	`SSLRequire not (%{SSL_CIPHER} in {"`*c1*`", ...})`	generalized
`SSLFakeBasicAuth`	`SSLOptions +FakeBasicAuth`	merged
`SSLCacheServerPath` *dir*	-	functionality removed
`SSLCacheServerPort` *integer*	-	functionality removed
Apache-SSL 1.x compatibility:		
`SSLExportClientCertificates`	`SSLOptions +ExportCertData`	merged
`SSLCacheServerRunDir` *dir*	-	functionality not supported
Sioux 1.x compatibility:		
`SSL_CertFile` *file*	`SSLCertificateFile` *file*	renamed
`SSL_KeyFile` *file*	`SSLCertificateKeyFile` *file*	renamed
`SSL_CipherSuite` *arg*	`SSLCipherSuite` *arg*	renamed
`SSL_X509VerifyDir` *arg*	`SSLCACertificatePath` *arg*	renamed
`SSL_Log` *file*	`SSLLogFile` *file*	renamed
`SSL_Connect` *flag*	`SSLEngine` *flag*	renamed
`SSL_ClientAuth` *arg*	`SSLVerifyClient` *arg*	renamed
`SSL_X509VerifyDepth` *arg*	`SSLVerifyDepth` *arg*	renamed
`SSL_FetchKeyPhraseFrom` *arg*	-	not directly mappable; use SSLPassPhraseDialog
`SSL_SessionDir` *dir*	-	not directly mappable; use SSLSessionCache
`SSL_Require` *expr*	-	not directly mappable; use SSLRequire
`SSL_CertFileType` *arg*	-	functionality not supported
`SSL_KeyFileType` *arg*	-	functionality not supported
		functionality not

`SSL_X509VerifyPolicy` *arg*	-	functionality not supported
`SSL_LogX509Attributes` *arg*	-	functionality not supported
Stronghold 2.x compatibility:		
`StrongholdAccelerator` *dir*	-	functionality not supported
`StrongholdKey` *dir*	-	functionality not supported
`StrongholdLicenseFile` *dir*	-	functionality not supported
`SSLFlag` *flag*	`SSLEngine` *flag*	renamed
`SSLSessionLockFile` *file*	`SSLMutex` *file*	renamed
`SSLCipherList` *spec*	`SSLCipherSuite` *spec*	renamed
`RequireSSL`	`SSLRequireSSL`	renamed
`SSLErrorFile` *file*	-	functionality not supported
`SSLRoot` *dir*	-	functionality not supported
`SSL_CertificateLogDir` *dir*	-	functionality not supported
`AuthCertDir` *dir*	-	functionality not supported
`SSL_Group` *name*	-	functionality not supported
`SSLProxyMachineCertPath` *dir*	-	functionality not supported
`SSLProxyMachineCertFile` *file*	-	functionality not supported
`SSLProxyCACertificatePath` *dir*	-	functionality not supported
`SSLProxyCACertificateFile` *file*	-	functionality not supported
`SSLProxyVerifyDepth` *number*	-	functionality not supported
`SSLProxyCipherList` *spec*	-	functionality not supported

Table 1: Configuration Directive Mapping

Environment Variables

When you use ‘‘`SSLOptions +CompatEnvVars`’’ additional environment variables are generated. They all correspond to existing official mod_ssl variables. The currently implemented variable derivation is listed in Table 2.

Old Variable	mod_ssl Variable	Comment
SSL_PROTOCOL_VERSION	SSL_PROTOCOL	renamed
SSLEAY_VERSION	SSL_VERSION_LIBRARY	renamed
HTTPS_SECRETKEYSIZE	SSL_CIPHER_USEKEYSIZE	renamed
HTTPS_KEYSIZE	SSL_CIPHER_ALGKEYSIZE	renamed
HTTPS_CIPHER	SSL_CIPHER	renamed
HTTPS_EXPORT	SSL_CIPHER_EXPORT	renamed
SSL_SERVER_KEY_SIZE	SSL_CIPHER_ALGKEYSIZE	renamed
SSL_SERVER_CERTIFICATE	SSL_SERVER_CERT	renamed
SSL_SERVER_CERT_START	SSL_SERVER_V_START	renamed
SSL_SERVER_CERT_END	SSL_SERVER_V_END	renamed
SSL_SERVER_CERT_SERIAL	SSL_SERVER_M_SERIAL	renamed
SSL_SERVER_SIGNATURE_ALGORITHM	SSL_SERVER_A_SIG	renamed
SSL_SERVER_DN	SSL_SERVER_S_DN	renamed
SSL_SERVER_CN	SSL_SERVER_S_DN_CN	renamed
SSL_SERVER_EMAIL	SSL_SERVER_S_DN_Email	renamed
SSL_SERVER_O	SSL_SERVER_S_DN_O	renamed
SSL_SERVER_OU	SSL_SERVER_S_DN_OU	renamed
SSL_SERVER_C	SSL_SERVER_S_DN_C	renamed
SSL_SERVER_SP	SSL_SERVER_S_DN_SP	renamed
SSL_SERVER_L	SSL_SERVER_S_DN_L	renamed
SSL_SERVER_IDN	SSL_SERVER_I_DN	renamed
SSL_SERVER_ICN	SSL_SERVER_I_DN_CN	renamed
SSL_SERVER_IEMAIL	SSL_SERVER_I_DN_Email	renamed
SSL_SERVER_IO	SSL_SERVER_I_DN_O	renamed
SSL_SERVER_IOU	SSL_SERVER_I_DN_OU	renamed
SSL_SERVER_IC	SSL_SERVER_I_DN_C	renamed
SSL_SERVER_ISP	SSL_SERVER_I_DN_SP	renamed
SSL_SERVER_IL	SSL_SERVER_I_DN_L	renamed
SSL_CLIENT_CERTIFICATE	SSL_CLIENT_CERT	renamed
SSL_CLIENT_CERT_START	SSL_CLIENT_V_START	renamed
SSL_CLIENT_CERT_END	SSL_CLIENT_V_END	renamed
SSL_CLIENT_CERT_SERIAL	SSL_CLIENT_M_SERIAL	renamed
SSL_CLIENT_SIGNATURE_ALGORITHM	SSL_CLIENT_A_SIG	renamed
SSL_CLIENT_DN	SSL_CLIENT_S_DN	renamed
SSL_CLIENT_CN	SSL_CLIENT_S_DN_CN	renamed
SSL_CLIENT_EMAIL	SSL_CLIENT_S_DN_Email	renamed

SSL_CLIENT_O	SSL_CLIENT_S_DN_O	renamed
SSL_CLIENT_OU	SSL_CLIENT_S_DN_OU	renamed
SSL_CLIENT_C	SSL_CLIENT_S_DN_C	renamed
SSL_CLIENT_SP	SSL_CLIENT_S_DN_SP	renamed
SSL_CLIENT_L	SSL_CLIENT_S_DN_L	renamed
SSL_CLIENT_IDN	SSL_CLIENT_I_DN	renamed
SSL_CLIENT_ICN	SSL_CLIENT_I_DN_CN	renamed
SSL_CLIENT_IEMAIL	SSL_CLIENT_I_DN_Email	renamed
SSL_CLIENT_IO	SSL_CLIENT_I_DN_O	renamed
SSL_CLIENT_IOU	SSL_CLIENT_I_DN_OU	renamed
SSL_CLIENT_IC	SSL_CLIENT_I_DN_C	renamed
SSL_CLIENT_ISP	SSL_CLIENT_I_DN_SP	renamed
SSL_CLIENT_IL	SSL_CLIENT_I_DN_L	renamed
SSL_EXPORT	SSL_CIPHER_EXPORT	renamed
SSL_KEYSIZE	SSL_CIPHER_ALGKEYSIZE	renamed
SSL_SECKEYSIZE	SSL_CIPHER_USEKEYSIZE	renamed
SSL_SSLEAY_VERSION	SSL_VERSION_LIBRARY	renamed
SSL_STRONG_CRYPTO	-	Not supported by mod_ssl
SSL_SERVER_KEY_EXP	-	Not supported by mod_ssl
SSL_SERVER_KEY_ALGORITHM	-	Not supported by mod_ssl
SSL_SERVER_KEY_SIZE	-	Not supported by mod_ssl
SSL_SERVER_SESSIONDIR	-	Not supported by mod_ssl
SSL_SERVER_CERTIFICATELOGDIR	-	Not supported by mod_ssl
SSL_SERVER_CERTFILE	-	Not supported by mod_ssl
SSL_SERVER_KEYFILE	-	Not supported by mod_ssl
SSL_SERVER_KEYFILETYPE	-	Not supported by mod_ssl
SSL_CLIENT_KEY_EXP	-	Not supported by mod_ssl
SSL_CLIENT_KEY_ALGORITHM	-	Not supported by mod_ssl
SSL_CLIENT_KEY_SIZE	-	Not supported by mod_ssl

Table 2: Environment Variable Derivation

Custom Log Functions

When mod_ssl is built into Apache or at least loaded (under DSO situation) additional functions exist for the Custom Log Format of mod_log_config as documented in the Reference Chapter. Beside the ``%{*varname*}x'' eXtension format function which can be used to expand any variables provided by any module, an additional Cryptography ``%{*name*}c'' cryptography format function exists for backward compatibility. The currently implemented function calls are listed in Table 3.

Function Call	**Description**
`%...{version}c`	SSL protocol version
`%...{cipher}c`	SSL cipher
`%...{subjectdn}c`	Client Certificate Subject Distinguished Name
`%...{issuerdn}c`	Client Certificate Issuer Distinguished Name
`%...{errcode}c`	Certificate Verification Error (numerical)
`%...{errstr}c`	Certificate Verification Error (string)

Table 3: Custom Log Cryptography Function