Cisco SSL Encryption Utility

- SSL Encryption Utility, on page 1

SSL Encryption Utility

Important Although this utility currently has its original name, the SSL Encryption Utility now configures web servers for use with TLS.

Unified CCE web servers are configured for secure access (HTTPS). Cisco provides SSL Encryption Utility (SSLUtil.exe) to help you configure web servers for use with TLS.

Note The SSL Encryption Utility is supported on servers running Windows Server.

Operating system facilities such as IIS can also accomplish the operations performed by the SSL encryption utility; however the Cisco utility simplifies the process.

SSLUtil.exe is located in the <ICMInstallDrive>\icm\bin folder. You can invoke the SSL Encryption Utility in standalone mode or automatically as part of setup.

The SSL Encryption Utility generates log messages pertaining to the operations that it performs. When it runs as part of setup, log messages are written to the setup log file. When the utility is in standalone mode, the log messages appear in the SSL Utility Window and the <SystemDrive>\temp\SSLUtil.log file.

The SSL Encryption Utility performs the following major functions:

- SSL Configuration
- SSL Certificate Administration

TLS is available for Unified CCE web applications installed on Windows Server. You can configure Internet Script Editor for TLS.

TLS Installation During Setup

By default, setup enables TLS for the Unified CCE Internet Script Editor application.

Note You must restart the SSL Configuration Utility if you use IIS manager to modify TLS settings while the utility is open.

The SSL Configuration Utility can be used to create self-signed certificates, to install the certificates in IIS, and to remove certificates from IIS. When invoked as part of setup, the SSL Configuration Utility sets TLS port in IIS to 443 if it is found to be blank.

To use TLS for Internet Script Editor, accept the default settings during installation and the supported servers use TLS.

During setup, the utility generates a self-signed certificate, imports it into the Local Machine Store, and installs it on the web server. Virtual directories are enabled and configured for TLS with 256-bit encryption.

Note During setup, if a certificate exists or the web server has an existing server certificate installed, a log entry is added and no changes take effect. Use the utility in standalone mode or use the IIS Services Manager to make certificate management changes.

Encryption Utility in Standalone Mode

In standalone mode, the SSL Configuration Utility displays the list of Unified ICM instances installed on the local machine. When you select an instance, the utility displays the installed web applications and their SSL settings. You can then alter the SSL settings for the web application.

The SSL Configuration Utility also facilitates the creation of self-signed certificates and the installation of the created certificate in IIS. You can also remove a certificate from IIS using this tool. When invoked as part of setup, the SSL Configuration Utility sets TLS port in IIS to 443 if it is found to be blank.

Transport Layer Security (TLS) Requirement

Contact center enterprise solutions use Transport Layer Security (TLS). Refer to your browser's documentation for details on how to configure support for TLS. See the Contact Center Enterprise Compatibility Matrix at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html for the supported TLS versions.

Note For backward compatibility with the earlier versions of clients, you can downgrade the Unified CCE Windows systems to earlier versions of TLS by following Microsoft procedures.

If you apply security hardening without configuring support for TLS, your browser cannot connect to the web server. An error message indicates that the page is either unavailable or that the website is experiencing technical difficulties.