CorreLog®

Apache TLS / Crypto
Enhanced Encryption Software

http://www.correlog.com   mailto:info@correlog.com

CorreLog, Enhanced Encryption Software Manual

Table of Contents

Section 1: Introduction

This manual provides supplemental information on how to enhance internal security of the CorreLog server by implementing Apache TLS and SSLv3 security for the web interface, and implementing secure encryption of message communication between CorreLog and its agent programs.

The software described in this manual adds extra internal security for data processing, needed for sites that require verifiable and published cryptographic algorithms. These sites may include government installations constrained to follow FIPS regulations, sites that require PCI/DSS certification, as well as sites that transmit information over the public Internet.

Prior to installing the Enhanced Encryption Software, you may wish to review this section to determine whether TLS and message encryption is actually needed at your site. CorreLog contains a number of security and encryption features without any special software described here. These core security features include encryption of data using a secure (but non-published) encryption algorithm, and various methods of authenticating users.

NOTE: The United States government regulates the export of cryptographic algorithms. Only parties known to and designated by CorreLog, Inc can use this product. For precise information on United States cryptography export/import laws, contact the Bureau of Export Administration (BXA) (http://www.bxa.doc.gov/). Or contact CorreLog, Inc. for more information.

Enhanced Encryption Software Description

This manual documents the "Apache TLS / Crypto Enhanced Encryption Software for CorreLog Internal Security" (herein referred to as the "Enhanced Encryption Software".) This package is provided as a separate download and add-on to CorreLog, and is not part of the native CorreLog distribution. The Enhanced Encryption Software is available only to CorreLog licensees.

The CorreLog Enhanced Encryption Software package adds a new Apache server to the system that supports HTTP TLS, and SSLv3. This package additionally enables encrypted transfers between CorreLog agents and the main CorreLog site, and other security functions documented in this section.

The user can follow the instructions in Section 2 of this manual to install the Enhanced Encryption Software package. Section 3 of this manual provides detailed information on how to configure message encryption by means of a secure upload protocol. Section 4 of this manual provides additional information on how to configure the Apache TLS functions.

Standard CorreLog Security Features

The CorreLog system employs basic data protection and secure processing, even without installing the Enhanced Encryption Software:

- **Authentication Of Users.** The basic CorreLog software uses message digests to authenticate users. Only users registered on the system may access or view CorreLog data.

- **Role Based User Permissions.** The basic CorreLog software allows users to be assigned to "guest", "user", and "admin" roles to govern what data a user may view or modify on the system.

- **Encryption of Data.** The basic CorreLog software encrypts passwords and other data on the disk using a robust (but unpublished) encryption algorithm. Additionally, CorreLog agents send data to the main CorreLog console in encrypted form.

- **Authentication During Remote Configuration.** The basic remote configuration function of CorreLog agents incorporates authentication by means of an encrypted passkey, and by source address, preventing unauthorized reconfiguration of agents.

- **Secure TCP Tunneling Software**. The basic CorreLog software system includes TCP tunneling software that encrypts data transfers, and also permits access to remote locations through a single TCP port.

Note that these features, documented in detail within other CorreLog manuals, may be adequate for many installations. Prior to implementing the TLS / Crypto software at a CorreLog site, administrators should consider whether these basic security features are adequate to meet the security policies of the organization.

CorreLog TLS / Crypto Features

In addition to the native CorreLog security features, the TLS / Crypto software increases the data processing security at the CorreLog site by adding extra encryption. Specific features of the Enhanced Encryption Software are as follows.

- **Authentication and Encryption of HTTP Requests.** The Enhanced Encryption Software adds a secure HTTPS server to the CorreLog site, so that all data transfers between a user's browser and the CorreLog server are authenticated and encrypted using standard TLS, SSLv3. This extra software includes elements needed to make a self-signed security certificate for the CorreLog installation.

- **Encryption of Agent Data Transfers.** The Enhanced Encryption Software enables encryption to CorreLog agent programs, which supplements the native encryption features of the agent programs with published and verifiable security.

- **Secure Key Upload Protocol.** The Enhanced Encryption Software adds a secure upload protocol, which allows easy maintenance of cryptographic keys, and furnishes the ability to periodically upload keys to CorreLog agents so as to promote secure operation.

- **Optional SSPI (Active Directory) Authentication of Users.** The Enhanced Encryption Software supports Microsoft's Security Support Provider Interface (SSPI), which the administrator can optionally configure so that CorreLog Server logins are authenticated against Active Directory rather than the internal database. This permits passwords to be stored in Active Directory, for easier maintenance of CorreLog user identities.

General Security Policies

Installation of the Enhanced Encryption Software is not adequate to guarantee site security. The software is just one part of a more comprehensive security strategy that must be employed within the organization, as follows:

- **Limiting Access To Secure Platforms.** The security of the CorreLog software depends upon employing good protection at each platform executing the software. Only designated users should be permitted to log

on to the computer executing the CorreLog, and on to those computers executing the CorreLog agent.

- **Physical Security.** The physical security of the hardware and platforms should be monitored, such as by implementing secure pass codes to network operation centers, implementing tamper resistant locks and seals, and limiting physical access to network devices.

- **Security Awareness.** A published security policy should be created by the organization, and all systems users should regularly review that policy. It may be helpful to designate a data security officer, who will promote security awareness, audit security policy compliance, and protect cryptographic keys and modules against unauthorized access.

The above policies are required as part of any security solution. It is a common mistake of users to assume systems are actually made secure through merely implementing data encryption. In fact, implementing the Enhanced Encryption Software package without providing physical security may actually make systems more vulnerable than before, since the Enhanced Encryption Software provides an illusion that the system is fully protected when in reality it is not.

Maintaining good security practices and safeguarding confidential information is the responsibility of everyone in an organization. Administrators can enhance security by implementing good policies and practices, such as enforcement of strong passwords, and monitoring system security (such as with the CorreLog Security Server). However, secure operation ultimately derives from vigilant monitoring of system security by all parts of the user community.

Section 2: Software Installation

This section provides a detailed procedure for installing the Enhanced Encryption Software at the main CorreLog site. Subsequent sections discuss the configuration and usage of this software after installation.

The Enhanced Encryption Software is obtained as a single self-extracting WinZip package from CorreLog, Inc. The user should verify this package comes directly from CorreLog, Inc., and not from any third-party.

The Enhanced Encryption Software package is executed on the CorreLog platform using an administrative login. As a precondition to installation, the main CorreLog software should already be installed and should be operating properly. Note that the existing CorreLog installation is required, and the Enhanced Encryption Software cannot be installed at a site where the basic CorreLog installation is also installed.

When the user executes the Enhanced Encryption Software Package, the package extracts files to the CorreLog directory, and then starts a setup wizard, described here. The user executes the wizard to completion, which will install all software elements and services needed to begin the configuration described in Section 3 of this manual.

Enhanced Encryption Software Installation Procedure

The procedure for installing the Enhanced Encryption Software package at an existing CorreLog site is provided below.

1. Log into the platform executing the main CorreLog server using an administrative login.

2. Copy the Enhanced Encryption Software package on to the platform. Verify that this is the precise package obtained from CorreLog, Inc. (If necessary, you can use the MD5 signature for the software package, obtained from CorreLog, Inc.) The name of this package will be co-N-N-N-tls.exe, where "N-N-N" is the version number for the package.

3. Execute the package. The package will display the version number and build date for the software, such as shown below.
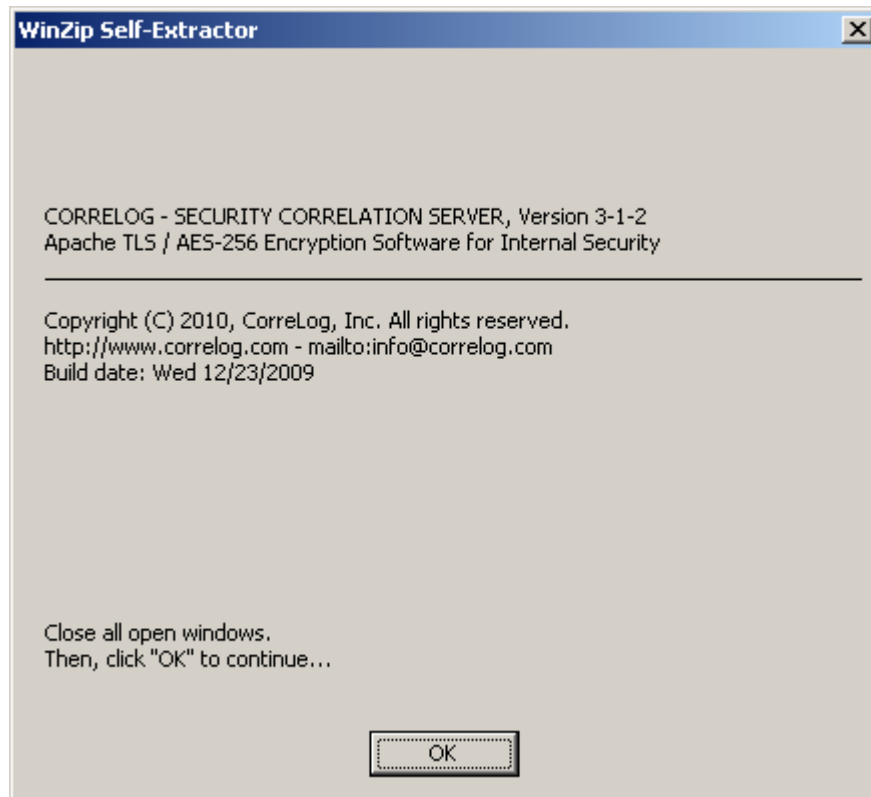

4. Click "OK" to close the version number screen, and then click "Unzip" to unzip files to the CorreLog root directory.

    Comment: Before unzipping files, the user should adjust the location of the "Unzip to folder" value to be the precise location where CorreLog is currently installed. The actual location may vary depending upon where

CorreLog was originally installed. You may determine the install directory for CorreLog via the web interface, using the "More > SysInfo" menu item at the upper right of the CorreLog web display.

Comment: If you are unable to extract files and receive a message indicating that the CO-apache-tls.exe program is busy, this is because you are re-installing the program, and the CO-apache-tls.exe program is busy. In this case, stop the "CorreLog Apache TLS" service via the Windows Service Manager, and then extract files.

5. After files are extracted, the Windows Setup Wizard automatically starts, depicted below. Click "Next >" to go to the next screen.
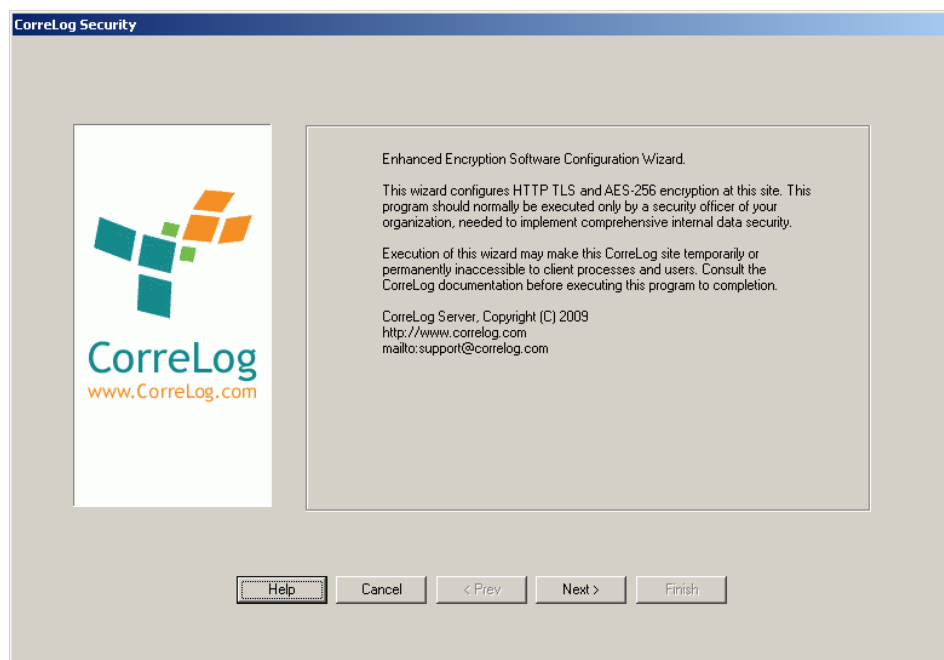
6. On the second screen of the Setup Wizard, the user is prompted for a Cipher Key Seed. The user should enter in random information at the keyword, ranging from 8 to 32 characters. This will form the basis of the encryption that is unique to this CorreLog site. The key does not have to be remembered or stored, and will not be recoverable by the user. The value will strictly be used to insure a highly random encryption key for the message encryption.

Comment: The key must contain at least one upper-case letter, one-lower case letter, one punctuation mark, and one number. The user can typically just type letter keys and numbers at random, holding down and releasing the shift key needed to insure a variety of characters. The dialog checks the strength of the cipher key seed and will not permit the user to continue if the key is not sufficiently random.

7. On the third screen of the Setup Wizard, the user is prompted for the port number for the HTTPS server. The user should enter a value of 443 to use the standard port number, or select some other port number.

   Comment: The screen selects a number for the user based upon the available free service ports on the system. The specified service port must be free from other programs. The dialog checks to verify that the port number is available and will not permit the user to continue if the port number specified is currently in use.

8. On the fourth screen of the Setup Wizard, the user is prompted for identity information needed to create the security certificate for the Apache server. The user can use the defaults, or can fill in a different company name, e-mail address, and website server name.

   Comment: The only critical field for this dialog is the "Common Name" for the certificate, which must precisely agree with the name of the device used in the URL when accessing the agent. This will only be an issue if users access the CorreLog server using some other name than the configured host name. For example, if the hostname for the CorreLog server is "correlog" but the official DNS name is "www.correlog.com" then users will receive a warning about the certificate when accessing the platform.

9. After entering the certificate information, the user can finish the wizard by clicking the "Next" and "Finish" buttons. The Apache TLS server will be automatically installed and started, and the Enhanced Encryption Software will be ready for configuration.

Installation Checkout and Verification

After installing the CorreLog software, the user should be able to immediately access the CorreLog server using HTTPS rather than HTTP. The user can specify the URL for the CorreLog server, and the website should appear.

Comment: A warning will also appear the first time the website is accessed, indicating that the certificate is unknown. The user can remove this warning message as described in Section 4 of this document.

If the user cannot access CorreLog via the HTTPS URL, then the "CorreLog Apache TLS" service may not have been properly installed or started. The user can troubleshoot this problem as follows.

1. Verify that the "CorreLog Apache TLS" service entry exists in the Windows "Control Panel > Admin Tools > Services" screen. If this entry does not

exist, then the service installation failed. Contact CorreLog support for assistance.

2. Verify that the "CorreLog Apache TLS" service was properly started. Run the Windows Task Manager. The "CO-apache-tls.exe" program should appear as a running process. If this process is not running, change working directories to the "CorreLog\apache-tls\bin" directory and try executing the CO-apache-tls.exe program at a command prompt. Inspect the command output for obvious permission errors.

3. Use the "netstat –a –n –p tcp" program at a command prompt and verify that the service port specified in screen three of the setup wizard is listening for requests. If the port number is listening, and the CO-apache-tls.exe program is running, then a firewall or proxy issue is preventing access to the CorreLog program. Review this problem with network administrators at your site.

4. Inspect the "logs\error.log" file for error messages. Contact CorreLog support for assistance, and be prepared to send this log file for analysis as needed.

Site Certificate Installation

Once the Apache TLS server is installed, and the user can access the CorreLog program via secure HTTPS, the website access is effectively encrypted. Errors dealing with the site certificate will have no affect on the actual encryption of data transfers to and from the server.

To prevent certificate notification errors, users can optionally import the site security certificate. This does not affect the encryption of data, but is strictly associated with authenticating the particular CorreLog site. For example, properly identifying and importing the site security certificate prevents a malicious user from "spoofing" the IP address of the CorreLog server and capturing the user login names and passwords used to access CorreLog. This may or may not be a likely attack scenario for your organization's private intranet.

The import process for HTTP site certificates is browser dependent. On Internet Explorer, users can import a certificate via the "Certificate Import Wizard" tool, available via the "Tools > Internet Options > Content > Certificates" screen, and also accessible via other locations within the Windows system.

Further notes on configuring message encryption and HTTP TLS software are provided in the sections that follow, and in the Appendix to this manual.

Configuration of Agent Encryption

The Apache TLS server includes capabilities to encrypt the agent-to-server message encryption. This feature requires no additional software installation, and specific steps regarding the configuration of this capability are documented in the next section of this manual.

Configuration of SSPI (Active Directory) Interface

Once the Apache TLS server is installed the administrator can optionally configure the SSPI interface via direct edits of the Apache TLS configuration file (located in the "CorreLog\apache-tls\config\httpd.conf" file.)

Specific instructions regarding this configuration are found elsewhere in this manual, including Appendix A to this manual.

Configuration of the SSPI interface is completely optional, and permits the CorreLog Server user password to be authenticated against Active Directory. This simplifies the maintenance of passwords and user authentication for the server. Refer to Section 5 for specific information.

Section 3: Crypto Configuration

This section provides detailed procedures for configuring and maintaining the Enhanced Encryption Software component, used to encrypt messages sent by CorreLog agents. These procedures should be performed after installing the CorreLog Enhanced Encryption Software, and are required to guarantee proper encryption of data transfers between CorreLog agents and the master CorreLog server.

Note that, if these procedures are not used, then the agents will send data using the native CorreLog encryption. This native encryption, while very strong (based upon a robust pseudo one-time pad algorithm) is not published. Hence the CorreLog native encryption is not compliant with FIPS and other specifications that demand use of published algorithms, and use of unique cipher keys.

To achieve FIPS and other regulatory compliance, it will be necessary to configure the encryption as described here. This provides verifiable encryption of data, using encryption keys that are unique to the organization.

Note that this section deals strictly with the message encryption, used to protect communication between the agents and the CorreLog server. A discussion of TLS encryption, used to protect communications between the CorreLog server and the user browsers, is discussed in Section 4.

Uploading Keys From The CorreLog Server

Before any agent will send encrypted data, the agent must receive an encryption key from the main CorreLog program.

To update a CorreLog agent with an encryption key, the operator follows the procedure below. This procedure should be executed for each new and existing CorreLog agent.

1. Login to the main CorreLog web interface with an "admin" type login.

2. Go to the "Devices" screen, find the device to upgrade (such as with the screen filter) and click on the hyperlink for the device. This displays the device information screen for the agent, shown below.

   Comment: The user can click on the IP address hyperlink found anywhere within CorreLog to access the device information screen. The "Devices" screen (specified above) is just one way to access the device information for a device.

3. If the top of the display contains the "Edit Remote Config" hyperlink, proceed to step 5. Otherwise, the remote configuration editor must be enabled for the agent, as explained in step 4.

4. Click on the "Edit Device Info" hyperlink, then set "Enable Remote Config Editor" to "Yes", and save the data by clicking on the "Commit" button. This returns the user to the screen displayed in step 2.

5. Click on the "Edit Remote Config" hyperlink to access the remote configuration editor for the agent, which fetches the remote configuration for the agent. Then, click the "Directly Edit Remote Configuration" hyperlink. This screen is shown below.

   Comment: If the remote device is not a CorreLog agent, or if a firewall prevents communication with the agent at port 55514, then an error message is displayed when the user clicks on the "Edit Remote Config" hyperlink. In this case, the operator must first resolve this problem, such as by modifying a firewall or installing the CorreLog agent on the target platform.

6. Click on the "Upload / Update Cipher Key" button. This sends the key to the remote agent and returns the user to the screen displayed in step 2.

   Comment: The "Upload / Update Cipher Key" button appears on device information screens only when the Enhanced Encryption Software has been installed at the master CorreLog site, and only if the "Enable Remote Config Editor" switch has been set to "Yes".

When the agent receives the new key, it will send a message to the main CorreLog console, which will be displayed in the "Messages" tab. If the user does not receive this message immediately after the key is uploaded then the remote agent did not receive the key properly. Otherwise, the agent will report that it has accepted the new key via a Syslog message, sent to the CorreLog server. This is the main indication that the data is now being encrypted on the system.

Uploading Keys Using The Rsmconf.exe Utility

An alternative to remotely uploading a cipher key via the CorreLog web interface is to use the "rsmconf.exe" program, which is included in the main CorreLog server, within the "system" directory. This utility permits the user to perform remote configuration at a command line, possibly within a batch file. The "rsmconf.exe" program accepts various arguments, documented in the "Windows Tool Set" User Manual.

To upload a key, the user executes the following command at the CorreLog server, within the "system" folder of the CorreLog installation:

```
Rsmconf.exe -key (ipaddr) (passkey)
```

In the above command, the (ipaddr) value is the IP address of the remote CorreLog agent. The (passkey) value is the passkey configured for the agent in its configuration file as documented in the Windows Tool Set" User Manual. The "passkey" argument provides rudimentary security by forcing the user to enter a passkey qualifier known to the agent program. This passkey does not form the basis for any verifiable security, but is still useful in limiting access to the agent. The argument is required to execute the "rsmconf.exe" program and cannot be omitted.

The rsmconf.exe program must be executed on the CorreLog server, within the system directory, and with the correct passkey qualifier. Any variations to this will result in an error message displayed to standard output, or logged to the CorreLog server by the agent, or both.

The "rsmconf.exe" program is especially useful in performing batch configure operations, where the command is repeated multiple times within a Windows ".bat" file, needed to effect reconfiguration on many different platforms. This furnishes a way to automate the key update process for large numbers of CorreLog agents.

Generating New Encryption Keys

It is good practice to occasionally change the encryption key for the system, to insure that the existing encryption key has not been compromised. This can be accomplished with no loss of transmission data by following the procedure below.

1. On the platform executing the main CorreLog program, stop the "CorreLog Apache TLS" service via the Windows service manager.

   Comment: This will stop only the secure Apache server. The other CorreLog services will continue to operate as normal, and the CorreLog server will continue to log message data without interruption or loss of data.

2. On the platform executing the main CorreLog agent, change working directories to the "CorreLog\apache-tls\bin" folder. This folder will contain the "CO-secure.exe" program.

3. Execute the CO-secure.exe program, and supply new security parameters. This includes a new cipher key seed value on the second screen of the dialog. Execute the CO-secure.exe program to completion.

   Comment: When finished, the CO-secure.exe program will restart the "CorreLog Apache TLS" service, which was stopped in step 1 above. A new security certificate will have been created, along with a new cipher key.

4. Upload keys with each CorreLog agent using one of the previously stated procedures given in this chapter.

Auditing Agent Encryption Keys

The main CorreLog system retains the last 16 keys generated by the CO-secure.exe program, so that message received from any CorreLog Agent using obsolete keys will still be properly decoded.

The operator can tell whether an agent is using the latest key by accessing the "Device Information" screen (by clicking on the device IP address hyperlink anywhere in the system.)

The user can audit the values for all keys by clicking the "Audit All CorreLog Agent Encryption" hyperlink, found at the bottom of the "Devices" screen. From that screen, the user can see if the encryption key used by an agent is the latest key, and can upgrade the agent key by clicking on the "Edit" hyperlink for the agent. See the screen depicted below.
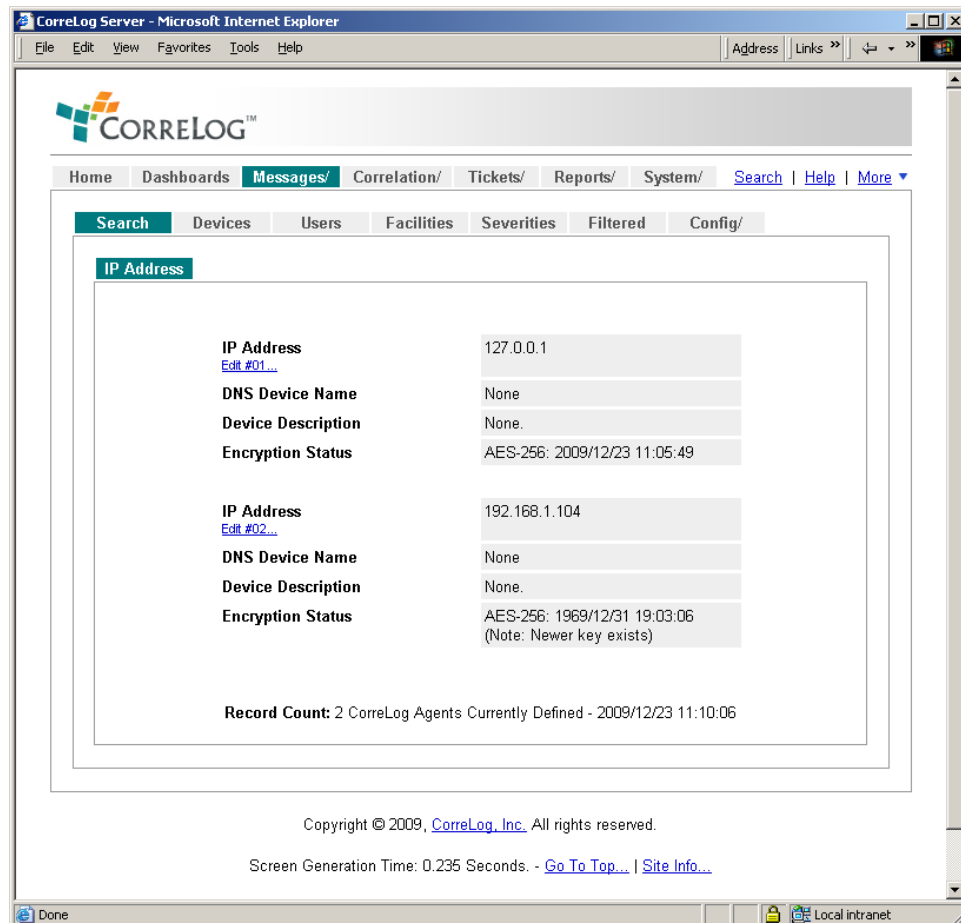
Manually Updating Encryption Keys

It may be desirable or necessary to manually transfer keys between the CorreLog master program and the remote agent programs. For example, a firewall may exist between the CorreLog agent program and the CorreLog server. In this case, the user can transfer the keys manually without using the Remote Configuration Facility. This procedure is as follows.

1. Log onto the main CorreLog server and change directories to the "CorreLog\config" folder.

2. Copy the "gparms.cnf" file, located in the "Correlog\config" folder, on to a removable disk.

   Comment: The specified disk or transport media should be FIPS compliant in order to maintain FIPS integrity. This may require observation of TEMPEST requirements, zeroing out of the removable media after transfer, destruction of the removable disk after transfer, or other specific site security policy requirements.

3. At the CorreLog agent installation, copy the "gparms.cnf" file to the same directory as the CO-sysmsg.exe program.

4. Edit the "gparms.cnf" file with a text editor, such as "notepad" and remove all but the top three lines of the file.

5. Save the "gparms.cnf" file as "CO-sysmsg.key", creating the file, or overwriting any existing file with the same name. Make sure the file is not accidentally saved with a ".txt" extension.

6. Stop and restart the CO-sysmsg.exe program via the Windows Task manager, or reboot the platform.

   Comment: The CO-sysmsg.exe program is controlled by the "CorreLog Message Service" entry of the Windows Service Manager. Stop and restart this service to force the CO-sysmsg.exe program to read the newly installed encryption key.

The "CO-sysmsg.exe" program looks for the "CO-sysmsg.key" file on startup, and reads this file to obtain the cipher key used for network transfers. The cipher key is encrypted in the file and cannot be decrypted by the user

Removing Encryption From An Agent

Once encryption is installed at an agent location, a manual process is required to remove the encryption.

1. Login to the platform executing the CorreLog agent, and change working directories to the location where the "CO-sysmsg" agent resides. This may be the "CorreLog\system" folder, or the "CorreLog\wintools" folder, or some other location.

2. Remove the "CO-sysmsg.key" file from the system. The user may wish to delete the file, or move it to a different name.

3. Stop and restart the CorreLog agent program. When the CorreLog agent program resumes it will no longer send encrypted data, and will revert to sending data using the native CorreLog encryption.

The "CO-sysmsg.key" file contains the encryption data for the agent. If the file does not exist, then the messages sent by the agent will contain only the basic encryption of the system. The user can send a new encryption key to the agent using the main CorreLog web interface, as discussed previously.

Testing The Encryption

The most basic test of encryption is to start (or restart) a CorreLog Agent and observe the startup message logged at the main CorreLog server. If the agent has operational encryption, the startup message for the agent will indicate encryption and the cipher key generation date as part of the logged message. This message itself is encrypted; hence if the CorreLog server correctly receives the message, then the end-to-end encryption is operational.

As a validation test, the CorreLog operator can also temporarily rename the "config/gparms.cnf" file at the main CorreLog server. This file contains the list of encrypted cipher keys. If the gparms.cnf file is not accessible, the CorreLog server will be unable to decrypt any received messages, and these messages will be logged using a "cdat://" prefix (indicating that the data could not be deciphered.) This verifies that agent programs are sending encrypted messages, and further allows auditing of the encrypted message.

Section 4: TLS Configuration

This section provides a discussion of the Apache TLS, SSLv3 component of the Enhanced Encryption Software. This component furnishes secure and authenticated communication between the CorreLog web interface and the user's browser.

The previous section discussed a customized encryption system, implemented for internal interprocess communication within CorreLog. Unlike that section, the use of SSL and TLS for HTTP is highly defined, standards based, and universally accepted. An abundance of public information exists on the Apache server and its secure configuration.

The Apache server provided with the CorreLog "Enhanced Encryption Software" is an especially hardened version of Apache, with most of its optional modules removed, and incorporating a predefined configuration created specifically to support CorreLog. There are several optional actions that can be taken in order to further tailor and configure the Apache TLS server, possibly to further strengthen the server, or provide special access depending upon the requirements of your enterprise. These optional steps are discussed in this section.

Note that this section deals strictly with the Apache TLS encryption, used to furnish secure communications between the CorreLog server and the user browsers. A discussion of message encryption, which secures the communication between CorreLog and its agents, is discussed in the previous section.

Apache TLS Process and Files

The Apache TLS software resides in a new CorreLog directory, at the pathname "Correlog\apache-tls". This directory follows the Version 2 directory structure, with the following subdirectories.

Apache-tls\bin

    This directory contains the Apache executable modules and required DLLs, including the openssl.exe utility, a batch file for creating certificates, and the CO-secure.exe CorreLog configuration wizard.

Apache-tls\conf

    This directory contains the Apache configuration files. In particular, this directory contains the "httpd.conf" file, which is the central configuration file for this version of the Apache server, documented online at a variety of websites.

Apache-tls\doc

    This directory contains special documentation for the Apache server, including a copy of this manual.

Apache-tls\install

    This directory contains special installation files. These files are used by the CorreLog configuration process and should not be edited or modified. (Changes to these files may break the CO-secure.exe setup wizard.)

Apache-tls\logs

    This directory contains log files generated by the Apache TLS server. The directory contains the "access.log" and the "error.log" files, each of which are the standard log files for Apache servers, documented online at a variety of websites.

Apache-tls\modules

    This directory contains dynamically loaded Apache modules. Not all of these modules are actually loaded by the basic CorreLog configuration of Apache. The particular required modules are listed in the "httpd.conf" file. All other modules in this directory are optional.

Apache-tls\ssl

    This directory contains the SSL configuration files for the Apache TLS server, including the ".crt" site certificate.

The Apache executable module, residing in the "bin" directory, is given the name "CO-apache-tls.exe", to identify this process clearly in the Windows Task

Manager. There will normally be two copies of this process executing, servicing HTTP requests at the port number specified when configuring the program.

Removing Non-Secure HTTP

With the Enhanced Encryption Software installed, CorreLog will normally run two different Apache servers. The "CO-apache.exe" program will continue to listen to the standard port of 80 (or non-secure port specified during CorreLog installation.) The "CO-apache-tls.exe" program will listen at the SSL port of 443 (or secure port specified during the Enhanced Encryption Software installation).

In this configuration, four different Apache processes will execute at the CorreLog server and will be visible in the Windows Task Manager.

To further enhance security, the non-secure Apache server can be disabled, and prevented from starting when the node boots. The procedure for disabling this server is as follows.

1. Login to the server platform executing CorreLog and access the "Control Panel > Administrative Tools > Services" screen. (An administrative login will be required to access this screen.)

2. Locate the "CorreLog Apache" service in the list of services, stop the service, and set the startup mode to be "disabled"

3. Optionally, rename or delete the "CorreLog\apache" directory from the system to prevent this apache server from being manually started.

The above steps are sufficient to guarantee that the CorreLog server can only he accessed via an https:// type URL. Note that removing the non-secure Apache server may affect links and bookmarks of system users. These users will now need to access CorreLog exclusively with https:// rather than simple http:// URLs.

Permanently Redirecting HTTP to HTTPS

As a final and optional step, the administrator can uncomment the directives at the bottom of the "conf/httpd.conf" file to enable permanent redirection of all HTTP requests to secure HTTPS. This step can be used to preserve links or bookmarks, while still ensuring that no unsecured access exists at the server.

The directives to redirect an HTTP request to an HTTPS request are clearly marked towards the bottom of the "conf/http.conf" file, as follows.

```
Listen             80
<VirtualHost       *:80>
RewriteEngine      On
```

```
RewriteCond           %{SERVER_PORT} !^443$
RewriteRule           ^/(.*) https://%{SERVER_NAME}/$1 [L,R]
</VirtualHost>
```

The above directives, which use the standard Apache "rewrite engine" functions, are normally commented out of the configuration, so that the administrator must explicitly enable redirection. Note that this step may slightly reduce the security of the site by making the common port 80 available to users.

After making the above changes, the administrator should stop and restart the Apache TLS service to force the server to re-read the configuration file. The operator can then test the system by accessing the site with "http://", and verifying that the site redirects automatically to be "https://".

Limiting Access to the HTTP Server

Normally, the HTTP server is configured to accept requests from all users of the system. The httpd.conf file can be easily modified to restrict the range of users to specific IP addresses.

The "allow" and "deny" directives restrict access based on the host name, or host address, of the machine requesting a document. The "order" directive describes the order in which to apply these directives.

For example the following directives are used to restrict access to a single domain:

```
Order deny,allow
Deny from all
Allow from www.correlog.com
```

The above directives deny access to the CorreLog website from all users except those originating from the www.correlog.com domain, even if those users otherwise have a valid username and password to the CorreLog system.

Monitoring Server Log Files

The standard CorreLog installation monitors the HTTP server log for error messages. The user can also monitor the Apache TLS server using this same technique. To configure the local CorreLog Agent to monitor logs, the following lines can be inserted in the "system\CO-sysmsg.cnf" file.

```
LogFile               ../apache-tls/logs/error.log
LogName               Apache-TLS:
MaxSizeChange         10000
DefaultFacility       network
DefaultSeverity       error
```

The above lines, when appended to the bottom of the CO-sysmsg.cnf file, will be sufficient to log all error messages of the Apache TLS server. Further refinement can be applied using MatchKeyWord directives, as discussed in the CorreLog Windows Tool Set Manual.

More Information On Apache…

The Apache server contains a rich assortment of special directives to support special modules, processing, security features, and customization. Refer to the Apache website for detailed information:

http://httpd.apache.org/

The OpenSSL module, which provides the encryption services for the Apache TLS server, is also highly versatile. The "openssl.exe" program, provided as a standard CorreLog component within the "apache-tls\bin" folder, furnishes a powerful command line interface and command options that can be used to encrypt and decrypt files and create certificates. Refer to the OpenSSL website for detailed information:

http://www.openssl.org/

Contact CorreLog, Inc. for assistance or clarification on any part of this manual, or on special operating details of the Enhanced Encryption Software.

Section 5: SSPI Configuration

This section provides a discussion of the SSPI (Security Support Provider Interface) of the Enhanced Encryption Software. This component is included in the Apache TLS software, and permits the user to authenticate logins using Active Directory, or via the native authentication of the CorreLog Server Platform.

The SSPI interface can be configured by the administrator to simplify the maintenance of CorreLog users. Rather than having the Apache TLS server maintain the passwords for users, these passwords can be maintained using the enterprise implementation of Active Directory. This feature employs an open source Apache software module to perform the authentication.

Normally, when the user logs into CorreLog, the password for the user is checked against the internal password database maintained by the "System > Logins" screen. If the username and password is accepted, the server allows the user access to the system based upon the type of user configured on that screen.

With the SSPI module enabled, the CorreLog server operates as described above, except that the password is checked against the password configured by the server platform. (If the server platform authenticates against Active Directory, then the CorreLog server is checked against active directory as well.) The SSPI module is configured manually, and the steps in this section should be followed carefully to prevent the administrator from accidentally being locked out of the system if the SSPI interface is initially misconfigured.

SSPI Operation Overview

To use the SSPI interface, the user first configures the name of the user on the "System > Login" screen. This user name MUST exist within the CorreLog server, and be identical to the name of the user that accesses the platform. Also, the user name must include a valid permission for the server (such as "admin", "dashboard", "guest", etc.)

Given the above, several conditions must exist to permit the user access to the CorreLog Server web interface, once the SSPI module is installed (as described in the next section.)

1. The user must enter a valid Domain\User name AND password into the HTTP authentication dialog. (The dialog is displayed when the user accesses the CorreLog web interface.)

2. The user name must be configured in the "System > Login" section of the program, and a valid program access assigned to that user.

   Comment: Just the user name, without the domain name, is entered into CorreLog "System > Logins" screen. The domain name is used during login, and must be entered into the login screen, but only the user name is used to assign permissions and user preferences.

If the above conditions exist, the user is logged into the CorreLog web interface as normal. Otherwise, if either condition fails (i.e. if the username or password is not valid for the platform, or if the user is not configured within the CorreLog web interface) an error message is displayed, which indicates a bad login.

Note that the SSPI module verifies the username and password against the CorreLog Server platform. If the platform employs Active Directory as its authentication mechanism, then the username and password is checked there. If the platform uses some other authentication mechanism (such as Workgroups, or local policies) then the password is checked against that data.

SSPI Installation Procedure

Installation of the SSPI module is a manual process, as follows:

1. First, prior to any other configuration, add the administrator login to the "System > Login" screen. The administrator name should the exact name of the user that accesses the platform, without specifying any domain name. For example, if you typically log into the CorreLog Server platform (i.e. Windows interface) with the username "org\jsmith", then you should configure the name "jsmith" within the "System > Login" screen, with an

"admin" type login.

Comment: Failure to add a proper administrative login can lock the administrator out of CorreLog, requiring the administrator to temporarily disable the Apache TLS server in order to repair the situation.

2. After adding a valid user login to the CorreLog Server, edit the "CorreLog\apache-tls\conf\httpd.conf" file with a text editor to uncomment the SSPI directives. These directives are found around 105 of the configuration file. (Search for "SSPI" within the configuration file.) The configuration directives are shown below:

```
# SSPI Support.
# Uncomment below to use Windows authentication,
# This requires the mod_auth_sspi.so module to be
# available. Additionally, further adjustments may
# depend upon the authentication types available.

<Directory "@@ROOTDIR@@/s-cgi">
AllowOverride None
Order allow,deny
Allow from all
AuthName "CorreLog Framework SSPI Login"
AuthType SSPI
SSPIAuth On
SSPIAuthoritative On
SSPIOfferSSPI  Off
SSPIOfferBasic On
Require valid-user
</Directory>

# If the above is uncommented, also uncomment below
# for dashboard gadgets. This is required for
# dashboard components to display correctly.

<Directory "@@ROOTDIR@@/s-cgi/gadgets">
AllowOverride None
Order allow,deny
Allow from all
Satisfy any
</Directory>
```

Comment: Generally, no changes will be necessary to the configuration file except for removing the "#" characters from the file as shown above.

The values of @@ROOTDIR@@ are replaced in the configuration file with the installation folder of the CorreLog Server

3. Stop and restart the CorreLog Apache-TLS server (via the service manager) for the above changes to be read by the Apache server.

4. Log into the CorreLog Server using the same login to access the platform, INCLUDING the domain name, such as "MyOrg\jsmith".

    Comment: Note that the domain name portion of the user name is used only by the SSPI server, entered only into the browser prompt, and that the domain name is not included on the "System > Login" screen.

5. Verify that the user is correctly logged onto the system with the proper credentials. The user can verify his or her login via the "Menu > Sys Info" screen, which will correctly display the user name and permissions to the server.

Specifying the Domain or Device Name During Login

Note that the HTTP login prompt, generated by the browser, ONLY accepts a username in the form: (domain)\(user), If a valid domain name is specified, the domain must be configured on the CorreLog Server platform. That is to say, if the user is unable to log into the actual CorreLog Server platform using the specified credentials, then the user will not be able to log into the CorreLog web interface. Likewise, any user of the CorreLog Server platform can be configured to also use the CorreLog web interface.

If the CorreLog Server platform uses only local authentication, the (domain) portion of the user name can typically be substituted for the hostname of the server. For example, if a local administrator exists for the "mydev" device, then the user can log into the CorreLog server with the credentials: "mydev\Administrator", supplying the proper password for the administrator with that login. If an "Administrator" user is configured for CorreLog, then permission to the web interface will be granted.

Recovering the Administrative Login

If the administrator fails to correctly specify his or her user name to the CorreLog Server via the "System > Login" screen (as described in Step #1 of the above procedure), the administrator may be locked out of the system, without any ability to grant new logins or make administrative changes.

If that situation occurs, the administrator may be able to explicitly access the website at port 80, which allows a user to log into the CorreLog web interface using the predefined credentials of the server. The administrator can then specify

the correct user name via the "System > Login" screen.

If Port 80 has been disabled to prevent non-SSL logins (as documented earlier in this manual), the administrator will need to comment out the Apache-TLS directives uncommented above, stop and restart the CorreLog server, and then access the server using the standard credentials configured in the "Login" screen. As needed, the administrator may need to completely reset the password database as described elsewhere, or contact CorreLog support for assistance.

Configuring Default Access

As a special case, the administrator can assign a "default access" to the CorreLog web interface that can be used by a user without a specific login entry within the "System > Login" screen. This may be useful if the administrator wishes to grant "Ticket' or "Guest" access (or some other limited permission) based upon active directory only.

To configure the default access to the program, the administrator accesses the "System > Parms" screen and sets the value of "Default Access" to be "guest". (This value is typically set to "disabled", meaning that if the user fails to log into CorreLog, they have no access to the CorreLog web interface at all.) The default access should be used carefully. For example, setting the default access to "admin" will allow any user with an Active Directory login to a platform complete access to the CorreLog web interface.

More Information on the SSPI Apache Module

The SSPI module is provided by the Open Source "Source Forge" project, and is not a standard Apache module. This has several implications with regard to maintenance and usage of the program. The SSPI module is not well documented or supported. CorreLog maintains its own version of the module, which may not be compatible with other Apache servers, and does not necessarily support the publicly documented directives of the SSPI module.

For further assistance on the SSPI module, contact CorreLog Support. Public information on this module, in addition to being inconsistent, can introduce security risks to the CorreLog server. Consequently, developers or administrators should attempt no modifications to the SSPI interface documented herein.

For Additional Help And Information…

Detailed specifications regarding the CorreLog Server, add-on components, and resources are available from our corporate website. Test software may be downloaded for immediate evaluation. Additionally, CorreLog is pleased to support proof-of-concepts, and provide technology proposals and demonstrations on request.

CorreLog, Inc., a privately held corporation, has produced software and framework components used successfully by hundreds of government and private operations worldwide. We deliver security information and event management (SIEM) software, combined with deep correlation functions, and advanced security solutions. CorreLog markets its solutions directly and through partners.

We are committed to advancing and redefining the state-of-art of system management, using open and standards-based protocols and methods. Visit our website today for more information.

CorreLog, Inc.
http://www.CorreLog.com
mailto:support@CorreLog.com

Appendix: Security Certificates

The CorreLog Apache TLS server uses industry standard "security certificates" to authenticate connections to the server. These certificates are used to authenticate the site, so that the browser based user is sure that they are talking to the CorreLog server and not some "spoofed" version of the program. This prevents a malicious user from setting up a copy of CorreLog within the enterprise, and then redirecting DNS services to this false copy of CorreLog (a process commonly known as "spoofing".)

The actual mechanism supported by TLS is documented in a variety of locations, and can be described briefly as follows: (1) A user requests a CorreLog Server web page using "https://" in the URL; (2) The CorreLog server sends its public key and certificate back to the user's web browser; (3) The browser checks that the certificate was issued by a trusted party; (4) The browser notifies the user of any errors with the certificate or; (5) The browser generates an encryption key for the transmission back to the CorreLog Server, which is used in the remaining communication processes.

This Appendix provides additional notes on Security Certificates, including a description of the various files used by the system, as well as methods and techniques for managing security certificates for effective security management of the CorreLog Server web interface..

Security Certificate Concepts

CorreLog uses a "self-signed" certificate, generated by the CO-SECURE.exe program when the program is first installed. This certificate has no root authority, but can be trusted by the person who created the certificate, hence provides true authentication to end-users on a local intranet.

The "self-signed" certificate will cause the browser to issue a warning to the end-user the first time the URL is accessed. Although this warning is extremely important when browsing the public Internet, it is not particularly significant for devices that are known to be on the local intranet of an organization.

On the public Internet, this warning might indicate someone has spoofed your bank, your social network, your corporate account, etc., and you are talking to a computer other than the one you expect, probably to acquire your secret password, or obtain other secret information. In this general case, you should proceed with extreme caution, and contact your Internet Service Provider, or the owner of the website.

Installing and Importing Security Certificates

In the specific case of communicating with the CorreLog server on your private corporate network, each end-user should handle the browser-warning message as follows:

1. The first time that an end-user sees the warning about a "non-trusted root authority" for the site, the user should contact the CorreLog administrator, and verify with that administrator the key is valid. (This step may be bypassed if the administrator has given the URL to the end-user, since presumably the CorreLog administrator has created and verified the certificate at that point.)

2. The end-user should add an exception for the site. This is browser dependent, but generally is accomplished using the "Options" tab of the browser to store the certificate in the "Trusted Root Certificate" store. This step will prevent any future errors from being displayed for that particular browser. (The process should be repeated for each browser for the end-user, i.e. for MS Internet Explorer, Firefox, Chrome, etc.)

3. If the warning message ever occurs again for this URL, the end-user should repeat the above steps. In particular, if the CorreLog administrator has not generated a new certificate, then the CorreLog site is probably being "spoofed" (as explained earlier) and the IP address should be tracked back to the person who installed the new copy of CorreLog within your organization.

Trouble Shooting Security Certificates

Note that when a certificate is generated, the administrator specifies the Common Name CN for the server, such as "clog-server", or "clog.domain.com", etc. This is the precise name that must be referenced as part of the "https://" URL when the CorreLog server is accessed. Otherwise, the common name will not match the URL, and the browser will flag the site as untrusted.

If a computer has more than one name, or if the CorreLog server is referenced by its IP address, then the URL will not match the Common Name and a warning will be generated as described above. Each certificate contains only one Common Name, and this name must agree with the value specified as the URL.

Before becoming alarmed about a "non-trusted root authority" warning, an end-user should verify that they are accessing the web site using the common name for the server, and not some alternate name for the server or the server IP address. This is a common mistake that is particularly easy to make on a local network where a device can sometimes be used without the fully qualified domain name, or via an IP address.

CorreLog SSL Certificate Directory

The "CorreLog\apache-tls\ssl" directory contains the security certificates and information related to the CorreLog Apache-TLS option. Pathnames to this folder and its various files are configured in the "CorreLog\apache-tls\conf\httpd.conf" configuration file of the CorreLog installation.

The "system\CO-SECURE.exe" program, launched when the Apache-TLS server is first installed, updates these files. These files may also be updated via the "bin\MAKE_CERT.bat" file, which provides an alternate method of generating security certificates using the OpenSSL.exe program.

Specific files supporting the Apache TLS server are as follows:

correlog.crt
> This file contains the security certificate for the site, created by the CO-SECURE.exe program or MAKE_CERT.bat file. This file is used to authenticate the system, and contains the "Common Name" CN for the server, authenticated by the user's web browser.

correlog.csr
> This file contains the "Certificate Signing Request" CSR for the site, which can be given to a certification authority in order to acquire a final certificate. (This file is not required, and provided for the convenience of the administrator.)

correlog.key
> This file contains the "Public Key Infrastructure" PKI key, which is used to encrypt data between the browser and the server. This file should generally not be distributed to third parties.

Generally, these files should be modified ONLY by the CO-SECURE.exe administrative tool, or via the MAKE_CERT.bat file. In some circumstances, the user may create or modify these files based upon third-party certifying authorities.

Additional Notes on Security Certificates

1. Security Certificates are generated by the system\CO-SECURE.exe program, which can be run at any time to create a new certificate for the user.

2. Security Certificates can also be run by the apache-tls\bin\MAKE_CERT.bat file, which provides an alternate way of generating security certificates via the "OpenSSL.exe" program.

3. Certificates, and other information (such as the certificate signing requests) reside in the "apache-tls\ssl" directory. The path to this directory is configured in the "httpd.conf" file of the installation.

4. End-users should import and store the CorreLog server certificate the first time that the CorreLog server is accessed. Subsequently, any warnings should be carefully investigated to see if the site is being "spoofed" by a malicious user.

5. Certificates contain the "Common Name" of the server, which must be included in the URL that accesses the server. Specifying a name other than the common name (including the IP address) as part of the URL will cause the browser to display a "non-trusted" status.

Alphabetical Index

A

U

Uncomment / 31
United / 5
Unzip / 10
Update / 18
Updating / 20
Updating, Manually Encryption Keys / 20
Upload / 7 18 19
Uploading / 16 18
Urls / 25
User / 6 18
Users / 6 7
Utility / 18

V

Verification / 12
Verify / 10 12 13 32
Version / 24
Visit / 34

W

Windows / 11 12 13 18 19 21 24 25 27 30 31
Winzip / 9
Wizard / 11 12 13
Workgroups / 30