



CorreLog Security Correlation Server, Installation Requirements

Hardware Requirements

For evaluations, CorreLog will run on a variety of Windows OS systems, ranging from Windows™ 200x, XP™, Vista™, and 7™, in as little as 512 MB of memory.

Listed below are our suggested recommendations for successfully installing and running a CorreLog Server in a production environment.

CorreLog Small Business Server

- 1 GB Memory
- Network Interface Card with static IP address
- 100 MB of disk storage for each day of logging*
- 20 MB storage for each day of archiving*

CorreLog Enterprise Server

- 4 GB Memory with dual processor
- High Performance Network Interface Card with static IP address
- 10 GB of disk storage for each day of logging*
- 2 GB of disk storage for each day of archiving* (generally on a network drive)

Software Requirements

CorreLog Small Business Server

- Windows 2003 or Windows 2008 Server
Windows XP or Windows Vista may be used for evaluation or small-scale systems
- Internet Explorer 7.0 or equivalent**
- Adobe Acrobat Reader***
- Apache Server (provided with installation)
- Microsoft Excel (optional reporting)

CorreLog Enterprise Server

- Windows 2003 or Windows 2008 Server
- Internet Explorer 7.0 or equivalent**
- Adobe Acrobat Reader***
- Apache Server (provided with installation)
- Microsoft Excel (for optional reporting)

* For a typical network, estimate 1 MB of message data daily per managed device. Actual usage may be more or less.

** Internet Explorer is recommended for client workstations. CorreLog is compatible with all popular browsers, but some minor features may require Internet Explorer.

*** Adobe Acrobat is required for viewing CorreLog's electronic documentation files and manuals.

Security And Access Requirements

A user must have Administrative rights on the CorreLog server platform in order to install and configure the software.

By default, the following TCP and UDP ports are used by the CorreLog Server system:

- TCP port 80 to support remote HTTP browsers
- UDP port 514 to receive standard SYSLOG messages
- UDP port 162 to receive standard SNMP Traps
- TCP port 51462 (optional), to support the CorreLog encrypted tunneling software

If you are running Virus Scan software on the CorreLog platform, you should exclude the CorreLog files from any on-access scanning, to prevent performance issues.

Syslog Messages

To receive Syslog messages from Windows 200X, Vista, and XP platforms, you must install the CorreLog Windows Tool Set software on each client platform. This is a standard part of the CorreLog installation software.

To receive Syslog messages from UNIX systems, root access to the client platform is required to configure the standard "syslog.conf" configuration file.

Windows Event Logs

Install the CorreLog Windows Tool Set on the client server(s) and/or workstation(s), as described in the CorreLog Quick Installation Guide.

SNMP Traps

Set the trap destination for the server, workstation or device to point to the CorreLog server.

Application Logs

Install the CorreLog Windows Tool Set on the client platforms and configure. (Contact CorreLog for platform compatible files, if needed.)

Other Notes

CorreLog is an extremely flexible system and supports many platforms not listed. In most cases, there are no hard stops during the installation due to hardware limitations. Contact CorreLog, Inc., and refer to the CorreLog System User Manual for more detailed information.

CorreLog Server, Frequently Asked Questions (FAQs)

How is the CorreLog system licensed?

CorreLog provides various licensing options including timed licenses, node-specific licenses and site-specific licenses. All licenses are installed by saving a text file (supplied by CorreLog support) in a system directory. The system automatically generates a 30-days license file on system installation.

Does CorreLog require you to install an agent on every server?

Correlog requires an agent only on Windows platforms. Native syslog, such as that supported by UNIX platforms, Routers, and application programs, does not require an agent or any software to install.

What types of data can CorreLog collect?

Correlog collects real-time syslog messages from Windows, UNIX, Cisco, and many other types of platforms. Additionally, Correlog will monitor streaming log files in any text format, including XML data, or Unicode data. CorreLog support Unicode and wide byte languages, such as GB2312.

What are the supported databases?

Correlog can support any ODBC compliant database. We recommend MS SQL or Oracle, but will work with access or other databases. Unlike many enterprise packages, CorreLog does not strictly require any particular database, and can work with no database installed or present.

How many Events Per Second (EPS) can the system handle?

A standalone Correlog server can handle between 2500 to 5000 EPS depending on the Hardware configuration. Four CorreLog servers can handle 10,000 EPS. The maximum theoretical limit for a two-tier server is 10 million EPS, collected across multiple CorreLog servers.

How do I know that my data has not been compromised or altered?

CorreLog automatically generates MD5 checksums on the log data and the MD5 is encrypted to prevent tampering. We also keep an audit trail to track all Correlog configuration changes. These elements are especially important for data forensics.

How secure are the login rules for the CorreLog admin account?

CorreLog employs HTTP authentication and encrypted HTTP. This is verifiable security. All passwords on the CorreLog server, including database passwords, are encrypted. Additionally, secure TLS and AES-256 option is available for domestic CorreLog customers.

Are there different levels of security in the CorreLog admin console?

CorreLog employs three permission groups: "admin", "user", and "guest". All users are assigned one of these roles when their login is created. All of these users can simultaneously use CorreLog, using their different permission sets.

How frequently will I get updates to the software?

The CorreLog server permits you to install one version on top of another version with no loss off data. Because agents use the standards based syslog protocol to communicate with the server, agents do not necessarily have to be upgraded. Software updates are available at the CorreLog website, along with release notes. A new version of CorreLog will be available every few months.

Can you bring all my archived data into the CorreLog server?

CorreLog has an import facility, which lets you migrate your data into CorreLog. The import facility provides an alternate way of bringing data into CorreLog for searching, correlation, and archiving.

How does CorreLog archive my log data?

CorreLog archives the log data each night, compressing the data and storing in a location specified via the CorreLog server web interface (such as external storage). Checksums are made on all data, and these checksums are encrypted to prevent tampering. Archives are restored via the CorreLog import program, discussed above.

Where can I get more information?

Check the CorreLog website at: www.correlog.com. In particular, check the "Resources" tab of the website, or contact CorreLog sales and support for detailed responses to your specific questions. We are always ready to discuss your applications for both licensed and evaluation versions of the program.