CorreLog, LDAP Interface Software Toolkit Manual

Copyright © 2008 - 2018, CorreLog, Inc. All rights reserved.

No part of this manual shall be reproduced without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibilities for errors or omissions. Nor is any liability assumed for damages resulting from the use of this information contained herein.
Table of Contents

Section 1: Introduction .................. 5
Section 2: Software Installation ............... 9
Section 3: Software Configuration ............... 13
Section 4: Software Operation ............... 19
Appendix: LDIFDE.exe Program .................. 27
Section 1: Introduction

This manual provides a detailed description of the CorreLog LDAP Interface Software (also known as the "CorreLog LDAP Tool Kit"). This is an optional set of files and executables added to the CorreLog Server that allows the CorreLog operator to interact with user definition data acquired directly from an LDAP server, including Microsoft Windows Active Directory.

The manual provides information on specific features and capabilities of this special software, including installation procedures, operating theory, application notes, and certain features not documented elsewhere.

The LDAP software can be installed at any CorreLog site. The software is not required by CorreLog to manage users, nor does it necessarily provide additional correlation functions within the program. The LDAP software provides utility in looking at external user data with application in forensics, and provides a convenient way of reading detailed user information that may be present in external data stores.

This manual is intended for CorreLog users who will operate the system, as well as system administrators responsible for installing the software components. This information will also be of interest to program developers and administrators.
Overview Of Operation

The LDAP Interface software more tightly integrates the CorreLog Server with an LDAP or Active Directory server. The software affects several screens as follows:

- System > Tools > Auto Update > LDAP Screen. The software adds a new "LDAP" tab to the "System > Tools" screen, allowing the manager to configure the LDAP acquisition process, schedule times to acquire LDAP data, and review the operation of the LDAP process.

- User Info Screen. The software adds a new "View LDAP Info" link to "User Information Screens" (accessed by clicking on a user name hyperlink anywhere within CorreLog.) This allows a system manager to view the LDAP records associated with a managed user.

- Messages > Users > Advanced" screen. The software adds new capabilities to the "Advanced" screen of the user monitor: (1) The operator can limit user discovery to only those names recording in the LDAP / Active Directory data, and the user can delete users that are not in the LDAP / Active Directory list.

Each of these capabilities is discussed in more detail within later sections of this manual.

LDAP Basics

Lightweight Directory Access Protocol (LDAP) is an application protocol for reading and editing information over a TCP/IP network. This information is often called a "directory", in that the information is organized into records of items.

Specifically, the information accessed by LDAP consists of a tree of directory entries, where each entry consists of a set of attributes and values. Each attribute has a specific name and one or more values. The attributes are defined in a schema appropriate for the particular directory name and attribute.

Each entry has a unique identifier referred to as its "Distinguished Name" (abbreviated "DN"), which is similar to the full pathname of a particular disk file. Users can query the DN, or a range of DNs.

Due to the flexibility associated with LDAP, and its overall security (implemented via TLS) it has become commonplace for organizations to keep user information in this type of directory. Microsoft Active Directory provides an extension to LDAP in that it can be used to authenticate users, hence providing a central mechanism for maintaining passwords, identifiers, and other items related to user logins.
A full discussion of LDAP is beyond the scope of this manual; LDAP is a well-documented protocol, and specifics related to all aspects of its use and operation are available from a variety of external sources.

How To Use This Manual

The next section of this manual (Section 2) provides the essential information needed to install the CorreLog LDAP Interface software. Note that several requirements exist to effectively use the software, documented in the next section.

The reader should review these constraints and requirements, as well as the functionality added by this software, to determine whether this software is suitable for installation at a particular site.
Section 2: Software Installation

NOTE -- As of Version 5-7-X, the LDAP adapter is a standard facility of the CorreLog Server, hence needs no special installation instructions. The information in this section is mainly useful for installing customized packages specific to customer sites, and the instructions in this section can therefore be ignored.

If needed, basic installation steps are as follows:

1. The operator obtains the CorreLog LDAP interface, in self-extracting WinZip format.
2. The operator stops the CorreLog Framework Service. (The LDAP package overwrites and replaces the CO-catlog.exe process; hence the CorreLog Framework Service cannot be running when this adapter is installed.)
3. The operator executes the self-extracting WinZip file. This unzips the software into the CorreLog Windows Distribution, including all configuration data and executables.
4. The operator restarts the CorreLog Framework Service.

Actual installation steps are documented in this section. The information needed to perform the configuration of the LDAP parameters is provided in Section 4. Specific application information (including usage information) is provided in Section 5. Note that administrative logins are required in order to perform the software installation, along with detailed information regarding LDAP server locations and capabilities.
Installation Requirements and Constraints

- **Existing CorreLog Server Installation.** Prior to installing the software, the CorreLog Server system must be installed on a Windows platform, as discussed in the CorreLog User Reference Manual.

- **Firewall Requirements.** The software requires that managed devices can access the target LDAP server. This may be a normal condition (however some sites may purposely disable this port, and those selected devices will not be manageable by CorreLog.)

- **Administrator Privileges.** The software requires an administrative login to the LDAP server to fetch information.

- **LDAP Directory.** The software requires that the user have an LDAP directory configured within the enterprise, such as Microsoft Active Directory or a UNIX LDAP implementation.

To insure proper installation of the program, the user should close all windows, and temporarily disable any port blocking or Virus Scan software on the system.

**Windows Installation Procedure**

The specific steps needed to install the software are as follows:

1. Login to the CorreLog Server Windows platform using an "Administrator" type login.

2. Stop the "CorreLog Framework Service" via the Windows Service Manager, or via the "net stop correlog" command at a cmd.exe prompt.

3. Obtain and execute the "co-n-n-n-ldap.exe" package, extracting files to the directory location where CorreLog is installed (by default the location "C:\CorreLog"). After extracting files, the "About" dialog is displayed indicating the success of the installation.

4. Restart the "CorreLog Framework Service" via the Windows Service Manager, or via the "net start correlog" command and a cmd.exe prompt.

5. Login to the CorreLog Server web interface, and verify that the "System > Tools > Auto-Update > LDAP" tab now exists.

If, after extracting files, you do not see the "LDAP" tab in the "System" tab, you probably extracted files to the wrong location in step #2 above. In this case, simply repeat the above procedure, extracting files to the correct installation folder for the CorreLog Server.
LDAP Parameter Configuration

Once the LDAP interface has been installed and is running on the system, the user can configure parameters associated with the interface. The user accomplishes this activity via the "System > Tools > Auto-Update > LDAP" screen. By default, all the user needs to do is to click the "Edit Button" and set the "Gen LDAP Enable" button to be "Enabled". The user may also generate new LDAP data on demand via the "Generate" button, and may set the execution time to be "Hourly", "Daily", or some other schedule of execution. Detailed options available to the user are described in Section 3 of this manual.

Third Part LDAP Browsers

The CorreLog LDAP interface is not intended to be a comprehensive LDAP browser. When configuring LDAP, it is often useful to deploy a third-party LDAP server on the CorreLog platform to verify connectivity and the "Distinguished Names" described in the next section. A variety of Third Party LDAP Browsers are available, many of them completely free.

In the absence of any specific preferences, CorreLog recommends the "Softterra LDAP Browser", which is available for download from the web, and easily located via any web search. This product, in addition to allowing easy browsing and troubleshooting of LDAP directories, implements an LDIF export utility that directly supports the format expected by CorreLog.

LDIFDE.exe Program

LDAP / Active Directory data is acquired by the CorreLog Server using the standard Windows "ldifde.exe" program. This utility is provided with CorreLog (and is also a standard part of modern Windows servers.)

Generally, no special configuration is required to begin using the LDIFDE.exe program, providing that the CorreLog Server is part of a Windows Domain. However, some instances may exist where the "gen-ldap.bat" file (in the "net-users" folder of the CorreLog Server) may need adjustments. For example, if the CorreLog Server node is not joined to a domain, or the administrator wishes to gather information from some Active Directory server in the organization, the "gen-ldap.bat" will have to be modified. This file exists in the following folder:

CorreLog\net-user\gen-ldap.bat

If special requirements exist for the installed site, contact CorreLog Support for assistance on modifying the above file, or consult web resources.
Section 3: Software Configuration

Once the CorreLog Server system is installed, the operator can configure and use the software in a variety of ways. Several parameters establish communications with the LDAP server:

- The operator should enable the GenLDAP program to run at some scheduled interval, such as hourly, daily or weekly. This is the single required setting change, necessary to start downloading and using LDAP / Active Directory data at periodic intervals.

- The operator may enable or disable settings in the "User Discovery" section of the browser, to limit discovered users to those that are contained in the LDAP / Active Directory listing. This feature cleans up the list of managed users, ensuring that a user name in CorreLog has a corresponding active directory element.

- The operator can delete users from the system who are not currently defined in the LDAP / Active Directory listing (possibly due to misconfigured discovery patterns, or due to local logons from the system.) This feature allows the CorreLog Administrator to quickly remove user entries that are not appropriate for the management activities.

Configuration of the system is not difficult, and several features are provided to check user input and perform tests. This section discusses the various parameters and steps necessary to configure a general purpose LDAP interface to CorreLog.
LDAP System Parameters Screen

As part of the Windows installation, a new tab is created in the "System > Auto-Update" section of the CorreLog web interface, which permits the user to configure various parameters associated with the LDAP background program. This screen is available only to CorreLog administrators, and serves as a starting point to configuring the LDAP interface. The LDAP parameter screen is depicted below.

The above screen allows the administrator to enable the Gen LDAP program (which causes LDAP data to be automatically downloaded) as well as allows the administrator to schedule execution of the program to be "Hourly", "Daily", "Weekly", or some other schedule defined in the "System > Schedule" screen. The above screen also allows the administrator to view various aspects of the LDAP data, or generate an LDAP listing on demand via the "Download" button.
Generate And Download Button

Once the LDAP parameters have been configured the operator must generate the actual LDAP data. This is accomplished by either waiting for the scheduled time, or by clicking the "Download" (or "Run Report") button at the top of the screen, which launches the "GenLDAP.exe" program as a background process on the system.

The "GenLDAP.exe" program gathers the LDAP data and formats the result into a file that is subsequently used by CorreLog. The data acquisition process may take several minutes or longer to complete, depending upon the number of LDAP data entries, the number of configured LDAP servers, and other factors. The process executes as a background process, and the user may leave the screen and return at a later time to check on the progress or the success of the operation.

Scheduling LDAP Queries

The "Generate" button permits the operator to regenerate the LDAP LDIF file on demand. However, it is usually desirable to execute these queries on a scheduled basis, such as once each day or each week. The LDAP screen provides controls to allow the operator to edit the scheduled execution. This can also be accomplished by configuring the "System > Schedule" screen to launch the GenLDAP.exe program at periodic intervals.

Include UPN Records

The LDAP parameters screen normally looks for "sAMAccountName" records to identify users. This operation can be extended by setting the "Include UPN Records" value to be "Yes", which looks for both "sAMAccountName" and "UserPrincipleName" records in the LDAP data.

This is useful for those sites that require the "UserPrincipleName" (UPN) for authentication and tracking of user activity.

The "Include UPN Records" setting is normally "No". Setting the "Include UPN Records" setting to "Yes" affects several parts of the program as follows:

- The list of active directory users (such as in the "Messages > Catalogs > Users" tab) will include both "sAMAccountName" and "UserPrincipleName" values (if the values are different.)

- When accessing the "User Info" screen (by clicking on the hyperlinked user name anywhere it appears in CorreLog) the "sAMAccountName" and "UserPrincipleName" values are displayed (if they are defined for the
This permits the operator to easily view the different identities associated with a particular user.

- If user discovery requires an LDAP match (as discussed elsewhere) then if a message matches either the "sAMAccountName" or "UserPrincipleName" fields, the user is discovered and added to the system. (See section below: "Limiting User Discovery To LDAP Users.")

- If the operator has implemented the "MemberOf" list macro, as discussed in the next section, then both the "sAMAccountName" and "UserPrincipleName" values are associated with the list macro generated by this facility.

Note that the "UserPrincipleName" value never includes the portion of the name trailing the "@" character. This makes the user name consistent with CorreLog naming conventions, but may cause problems for users with the same name spanning different domains (because the "@dom" value is omitted.)

**Edit MemberOf List Macro Update Rules**

The LDAP parameters screen includes a special "Edit MemberOf" button, which allows the administrator to configure up to eight different match patterns that can automatically create group membership lists. This allows the system to automatically create, maintain, and update lists of users that share a similar LDAP group membership.

When the LDAP information is downloaded, this information is automatically parsed to create a list of users that belong to the specified group(s). Any existing lists are replaced with the new information.

These lists appear on the "Correlation > Config > Lists" screen, and are identical to other lists that come with the system, except the lists reflect LDAP user names that belong to a particular set of Active Directory groups.

One application of this function would be to automatically create a list of administrators that belong to the "Administrator" group, so that this list can be used in reports, correlation rules, and alerts. The "Edit MemberOf" function is documented in the next section.

**Edit User Info Settings**

As a special function, the administrator can configure the system to automatically update "User Information" screens directly with Active Directory information. The user clicks on the "Edit User Info Update Settings" button at the bottom of the screen to view or adjust these settings. Generally, no changes are usually
necessary to this screen. (The screen mainly exists to extend this facility to non Active Directory LDAP installations.)

The user information appears when the operator clicks on any user name in CorreLog Server. The default action of this facility is to "Merge" user information with the existing information, i.e. to assign a full name (and other information) to users that do not have an existing name assigned to them. The full name then appears on the "Messages > Catalogs >Users" screen (and appears in other locations.)
Section 4: Software Operation

The LDAP interface tool kit extends the range of CorreLog to allow easy access to the registered and "official" user information of the enterprise. This user information is stored on the system, and is available from various CorreLog screens to display or process information related to a user.

Although the software does not provide any direct correlation functions, the user can compose "Custom Alert" scripts (and other software, such as "Correlation Actions") that access the local LDAP server data and perform user define correlation, such as capturing the counts for groups of users with certain common LDAP parameters (such as the same group or domain.)

Additionally, the LDAP toolkit incorporates several features to work with the "User Discovery" process of the server, and will limit the list of users to those that are defined in the LDAP file. Also, the operator can get a list of users that are not currently defined in the LDAP listing, assisting in the management and maintenance of the user list.

This section provides a description of the various optional software elements, their operation and other considerations, including screenshots.
LDAP LDIF List File

The main purpose and intent of the LDAP interface software, discussed to this point (including the configuration items of Section 3) is to create an LDAP Data Interchange Format (LDIF) file on the CorreLog system.

The LDIF file is a standards-based text file that consists of multiple "attribute / value" pairs, where the first token of the file represents an LDAP attribute, and the remainder of the line represents the attribute's value. The file can be very large, depending upon the number of managed users. A file of over 100 Mbytes or more is quite typical.

Actual attributes associated with LDAP can vary according to different LDAP schemas associated with platforms and organizations. For example, logon user names are often represented as either "sAMAccountName" attributes or "UserPrincipleName" on Windows systems, also represented as "Uid" values on UNIX systems. This makes the actual understanding of the LDAP and LDIF file somewhat difficult to users that are unfamiliar with the organization's conventions.

Fortunately, an abundance of information exists regarding LDAP attributes and their properties via web searches, and readers can often surmise the range of values for a particular LDAP attribute by simple inspection.

The LDIF file is synchronized to the user information found in the "net-user" directory, and can be used in a variety of ways. In particular the LDAP Interface Toolkit modifies the "User Info" screen so that the operator can drill down to a monitored user and view the LDAP information for the user. Other applications of the LDAP LDIF file (discussed in later sections) are also possible.

User Info Interface

The LDIF information is displayed via the "User Information" screen (which is accessed whenever the operator clicks on a user name hyperlink anywhere within CorreLog.) The "User Information" screen supports access to the LDAP data two distinct ways.

If the LDAP interface is installed on the system, a new hyperlink appears in the upper right of the "User Information Screen" display. If the "View LDAP Info" hyperlink is clicked, the current LDAP information for the user is displayed in a new screen.

The User Info interface screen, showing the "View LDAP Info" link, is displayed below. When the user clicks on the "View LDAP Info" hyperlink, the current LDAP information is displayed in raw form, depicted in a later section of this manual.
To view the LDAP information for any user, the operator first clicks on the "User Name", and then clicks on the "View LDAP Info" hyperlink. If LDAP information has been gathered for the user, the LDAP data is depicted in tabular format. This allows the operator to see detailed information about the users various characteristics, possibly including alternate phone numbers, login attempts, last login time, and other common LDAP values.
LDAP Info Screen

When the user clicks on the "View LDAP Info" hyperlink, on the "User Info Screen", the current LDAP data for the user is displayed in tabular format. The data may contain a combination of binary and textual data, and is sorted in the order returned by the LDAP server (typically the order in which the data was entered.) The user name can be changed via the "Apply" button. The operator can return to the "User Info" screen by clicking on the "Continue" button. The screen is depicted below.

![LDAP Info Screen](image)

Note that it is quite possible that a CorreLog monitored user is not in the LDIF file. For example, if the user is registered in some organizational unit other than those configured in the "System > Tools > Auto-Update > LDAP" screen, the user LDAP data will not be collected and clicking on the "View User Info" hyperlink will return an error. Further note that the LDAP data is also dependent on the particular Schema of the organization, so certain LDAP attributes may not exist on some platforms.
Limiting User Discovery To LDAP Users

After installing the LDAP Tool Kit software, the administrator can limit the discovery of users to those that are defined in the LDAP data, via a new select menu that is added to the "Messages > Users > Advanced" screen. By default, this must first be enabled by the administrator to begin processing information. (The button appears ONLY after enabling LDAP on the "System > Tools > Auto-Update > LDAP" screen.) This modification is depicted below.

As show above, the "Require LDAP User Match" field allows the administrator to require an LDAP User Match before a user is automatically added to the system. Specifically, when a user is discovered, the list of excluded user names is tested, followed by the LDAP user list. When "Require LDAP User Match" is "True", the user name must not be excluded AND must be in the LDAP list.
Removing Non-LDAP Users

After installing the LDAP Took Kit software, the administrator can easily remove any users that are not in the LDAP user list. This is accomplished via a new button added to "Messages > Users > Advanced > Delete Users By List" screen. This new button is depicted below.

As shown above, when the operator clicks the "Select Non-LDAP Users" button, the "Delete User Name List" is updated with a list of users that appear in the CorreLog "Users" tab, but do not appear in the LDAP data. The operator can then (optionally) edit the list and click the "Delete" button to delete the list of users. These actions will clean-up CorreLog so that only LDAP users are monitored.
Edit MemberOf Macro Values

As a special function, when LDAP data is acquired, the system can automatically update lists of users based upon match patterns for the "MemberOf" LDAP directive. This allows user lists to be automatically populated and maintained by the system, such as to maintain a current list of privileged users. This function is accessed via the "Edit" button on the "LDAP" screen, which displays the screen below:

![Screenshot of the Edit MemberOf Macro Values interface]

As shown above, the "Edit MemberOf" function provides eight different slots, permitting up to eight different list macros to be created and maintained by the system as follows: The user provides a List Macro name, and a match pattern that is applied to all "MemberOf" directives in the LDAP data. If the "MemberOf" string matches the pattern, then the user name is automatically entered into the specified list when LDAP data is acquired. This provides a simple way to automatically update and maintain lists of users that are available to the system.
Custom Alert Programs

As a final topic, it is worthwhile to discuss possible applications of the LDAP data on the system. This section has identified several built-in interfaces, but once the LDAP data has been placed on the system, various other applications also exist.

Specifically, an operator / programmer can create "Custom Alerts" that make use of the "gen-ldap" files, such as to acquire counts of all messages (possibly of a specific class) for users in a particular group, as identified by a common LDAP attribute. This count value can then be alarmed to detect when users within a particular group perform some operation over a specified limit. This may detect cases where groups of people are collaborating in stealing data or performing some unauthorized action.

Custom Alert programs are beyond the scope of this manual, and are documented elsewhere. However, with the LDAP LDIF data stored on the CorreLog server, it becomes possible to perform more advanced correlation and detection based upon the external data found in the LDAP server, opening many new possibilities in user anomaly detection and management not otherwise possible.
Appendix: LDIFDE.exe Program

LDAP / Active Directory data is acquired using built-in libraries, and installation of the LDIFDE program is not strictly required to use the LDAP interface.

HOWEVER, the "ldifde.exe" program, which is a standard Windows utility available on Windows 2008 and other systems, can be substituted for the internal libraries, as may be necessary in some customized installations. This Windows utility program is executed by the "CorreLog\net-user\gen-ldap.bat" file (launched via the "GenLDAP.exe" program.)

If necessary, an administrator may edit the "gen-ldap.bat" file to provide special directives or other logic needed to support the site. When the "gen-ldap.bat" file executes, the resulting raw LDIF list must be placed by the batch file in the location specified by the %LDAP_OUTPUT_FILE% environmental variable. When the batch file exits, the GenLDAP.exe program resumes its background execution and formats data into the expected and required files for the system.

The "ldifde.exe" program is well documented on the web. Additionally the operator can execute "ldifde.exe /?" for brief help on the various options available for configuration.

Note that the "gen-ldap.bat" file, described above, normally does not require any changes or modifications if the CorreLog Server domain is joined to the domain of the organization.
GenLDAP Batch File Environmental Variables

When the "gen-ldap.bat" file (residing in the "net-users" folder of the server installation) is executed, the batch file can access various environmental variables. This furnishes flexibility that may be necessary to add extra functionality or accommodate special conditions.

Environmental variables and values, instantiated prior to the system launch of the "gen-ldap.bat" file, are documented below.

- **%LDAP_CMD%** - This environmental variable is the pathname to the external command that actually gathers the LDAP information. This normally points to an external executable or DLL. The environmental variable can be replaced by the hardcoded path to "ldifde.exe" on the system, or some equivalent value. Note that "%LDAP_CMD% can change between server software versions.

- **%LDAP_OUTPUT%** - This environmental variable is the pathname to a temporary output file that contains the LDAP output. This value is typically the path ../net-users/gen-ldap.dat_tmp", but the value can change between server software versions.

- **%LDAP_OPTIONS%** - This environmental variable contains the name of the LDAP server (if configured and other than "Default"). The value is used as a command line argument to the %LDAP_CMD% value. (The value of the "LDAP Server Name" is configured on the "Edit" screen for the adapter.)

- **%LDAP_METHOD%** - This environmental variable reflects the settings configured on the LDAP Adapter "Edit" screen, after clicking the "Special Auth Settings" link. The value is whatever the operator has selected as the "LDAP Auth Method" on that screen.

- **%LDAP_USER%** - This environmental variable reflects the settings configured on the LDAP Adapter "Edit" screen, after clicking the "Special Auth Settings" link. The value is whatever the operator has selected as the "LDAP Auth User Name" on that screen.

- **%LDAP_PASS%** - This environmental variable reflects the settings configured on the LDAP Adapter "Edit" screen, after clicking the "Special Auth Settings" link. The value is whatever the operator has selected as the "LDAP Auth Password" on that screen. Note that the password is encrypted on the disk, and is generally not retrievable via the Web interface.
• %LDAP_DOM% - This environmental variable reflects the settings configured on the LDAP Adapter "Edit" screen, after clicking the "Special Auth Settings" link. The value is whatever the operator has selected as the "LDAP Auth Domain" on that screen.

One application of the above variables is to construct a "gen-ldap.bat" file that gathers information from various domain controllers, such as to support an enterprise with more than one domain. An example of such a modification is furnished below. The administrator can copy and paste the info below into the "gen-ldap.bat file, configure the domain names (replacing dname1 and dname2 below) to acquire data from two different domain controllers.

```
REM: # Acquire data from two domain controllers:
REM: # Each controller has a non-privileged user, whose
REM: # name and password are configured in the CorreLog
REM: # Server.

DEL %LDAP_OUTPUT_FILE% > NUL 2>&1
REM: # Get data from dname1
DEL tmp.txt > NUL 2>&1
%LDAP_CMD% %LDAP_OPTIONS% -b %LDAP_USER% dname1 %LDAP_PASS% -f tmp.txt
Type tmp.txt > %LDAP_OUTPUT_FILE%
REM: # Get data from dname2
DEL tmp.txt > NUL 2>&1
%LDAP_CMD% %LDAP_OPTIONS% -b %LDAP_USER% dname2 %LDAP_PASS% -f tmp.txt
Type tmp.txt > %LDAP_OUTPUT_FILE%
REM: Finished. Cleanup
DEL tmp.txt > NUL 2>&1
```

Note - these settings may be necessary depending upon your site's LDAP server security settings. If you receive an "SSPI Bind Error" indication in the "Process Log" of the LDAP screen, you may change the "LDAP Auth Method" below to be "LDAP-Logon", and then furnish a username, password, and domain name for the LDAP download operation. You many use a low-privilege user name below for the download operation. Information below is encrypted at this site.

Interested parties should consult web resources, or contact CorreLog Support for additional information.
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