



Tenable Log Correlation Engine Tenable Log Correlation Engine 6.0.x User Guide

Last Updated: November 07, 2023



Table of Contents

Welcome to Tenable Log Correlation Engine	9
Get Started	10
Components of the Tenable Log Correlation Engine	12
Hardware and Software Requirements	15
Install the Log Correlation Engine Server	21
Tenable Log Correlation Engine Server Installation	23
Quick Setup	24
Offline Activation and Plugin Updates	27
Shortcuts for Running SQL Commands and Scripts	30
SQL Scripts	32
dimension-occurrence-stats.sql	40
throughput--kilo-eps.sql	42
Files and Layout	43
Location of PostgreSQL Files in an Log Correlation Engine Installation	45
Tenable Security Center CV Integration	46
Add Tenable Log Correlation Engine to Tenable Security Center	47
Configure Organizations	49
Using Tenable Security Center with Tenable Log Correlation Engine	50
Analyzing Events	51
Full Text Searches	53
Queries Against Archived Snapshots	58
Health and Status	59
Feed	60



Statistics	61
Data Sensors	63
Alerts	64
Advanced	66
System Configuration	67
Basic Configuration	68
Storage Configuration	70
IDS Configuration	72
High Availability	74
Configure High Availability	76
Migrate Your High Availability Configuration to Log Correlation Engine 6.0.4 or Later	80
Migrate Your High Availability Configuration to Log Correlation Engine 6.0.5 or Later	83
Monitor Your High Availability Configuration	85
Disable High Availability	88
Advanced Configuration	89
Data Forwarding	101
Receiving Encrypted Syslog	105
Example Encrypted TCP Syslog Configuration	107
TASL and Plugins	111
Event Rules	112
Event Rules Examples	119
Service Control	121
Feed Settings	122
Feed Registration	123



Plugin Update	124
Web Proxy	125
Tenable Vulnerability Management Configuration	126
Refresh or Replace the Vulnerability Reporter SSL Certificate	127
Upgrade the Log Correlation Engine Server	129
Upgrade your Log Correlation Engine License	132
Users	133
Add Users	135
View User Accounts	136
Edit Users	138
Change a User's Password	139
Delete Users	140
Unlock a User Account	141
Lock a User Account	142
Certificate-Authenticated Web UI Logins	143
Configure Certificate-Authenticated Web UI Logins	144
Enable Certificate-Authenticated Web UI Logins for a User	145
Disable Certificate-Authenticated WebUI Logins	146
Manage Clients in Tenable Log Correlation Engine	147
Clients Page Tasks	150
Authorize an Tenable Log Correlation Engine Client	151
Additional Clients Page Tasks	152
Rename a Tenable Log Correlation Engine Client	155
Assign a Policy to an Tenable Log Correlation Engine Client	156



Assign an Tenable Log Correlation Engine Client to a Server	157
Revoke a Tenable Log Correlation Engine Client Authorization	158
Delete a Tenable Log Correlation Engine Client	159
Client Policies	160
Client Policy Builder	163
Create a Client Policy with the Client Policy Builder	165
Edit a Client Policy with the Client Policy Builder	168
Upload a Client Policy	170
Download a Client Policy	173
Clone a Client Policy with the Client Policy Builder	174
Other Policies Page Tasks	177
Delete a Client Policy	178
Automatically Authorize Tenable Log Correlation Engine Clients	179
Tenable Log Correlation Engine Clients	180
Tenable Log Correlation Engine Client for Windows	183
System Requirements	184
Install, Configure, and Remove	185
Download an Log Correlation Engine Client	186
Install the Tenable Log Correlation Engine Windows Client	187
Install the Log Correlation Engine Windows Client Remotely	188
Configure the Log Correlation Engine Windows Client	190
Windows Client Policy Configuration Items	191
Remove the Log Correlation Engine Windows Client	203
Tenable Log Correlation Engine Windows Client Features	205



Configure the Windows Client Policy	206
Tenable Log Correlation Engine Client for Linux	207
OPSEC Client	208
Get Started with the Tenable Log Correlation Engine Splunk Client	209
Install, Configure, and Remove	210
Install the Log Correlation Engine Splunk Client	211
Configure the Log Correlation Engine Splunk Client	212
Remove the Log Correlation Engine Splunk Client	214
Tenable Log Correlation Engine Splunk Client Features	215
Data Comparison	216
Configure Splunk	218
Configure Splunk to Forward Data	219
Configure the Splunk Client Policy	220
Additional Resources	221
Splunk Client Policy Configuration Items	222
Delimiters	229
Tenable NetFlow Monitor	231
Tenable Network Monitor	232
Tenable RDEP Monitor	233
Tenable SDEE Monitor	234
Get Started with the Log Correlation Engine Web Query Client	235
Hardware Requirements	236
Software Requirements	237
Licensing	238



Install, Configure, and Remove	239
Install the Log Correlation Engine Web Query Client	240
Configure the Log Correlation Engine Web Query Client	241
Remove the Log Correlation Engine Web Query Client	243
Features	244
Monitor Amazon Web Services (AWS)	245
Monitor Salesforce	246
Monitor Google Cloud Platform (GCP)	247
Monitor and Limit Bandwidth	248
Monitor Client Statistics	249
How To	250
How to Monitor Amazon Web Services (AWS)	251
Prerequisite Tasks for Integration with AWS	252
Configure the Web Query Client Policy for AWS	253
Review AWS Events in Tenable Security Center	255
How to Monitor Salesforce	257
Prerequisite Tasks for Integration with Salesforce	258
Configure the Web Query Client Policy for Salesforce	259
Review Salesforce Events in Tenable Security Center	261
How to Monitor GCP	262
Prerequisite Tasks for Integration with GCP	263
Configure the Web Query Client Policy for GCP	265
Review GCP Events in Tenable Security Center	268
Additional Resources	269



Web Query Client Policy Configuration Items	270
Correcting AWS Configuration Issues	279
Correcting Network Time Protocol Issues	281
WMI Monitor Client	283
Additional Resources	284
Tools	285
install-PostgreSQL-man-pages	297
ts-test	298
validate-prm-regex	301
Perform an Online PostgreSQL Backup	303
Restore an Online PostgreSQL Backup	304
Site Policies	305
Rotate Web UI Credentials	309
Encryption Strength	310
Configure TLS Strong Encryption	311
Configure Tenable Log Correlation Engine for NIAP Compliance	312
File and Process Allow List	314
Refresh or Replace the Vulnerability Reporter SSL Certificate	320
Import Log Correlation Engine Data Manually	322
Manual Key Exchange with Tenable Security Center	323
User Tracking	326
Non-Tenable License Declarations	328
Silo Archiving	329



Welcome to Tenable Log Correlation Engine

This document describes the installation, configuration, and administration of the Tenable **Tenable Log Correlation Engine**® (Tenable Log Correlation Engine®) Tenable Log Correlation Engine 6.0.x (formerly known as LCE) for use as a part of Tenable Security Center+.

Log Correlation Engine is used with Tenable Security Center, which is installed separately. This documentation assumes that you already have an operational instance of Tenable Security Center. Knowledge of Tenable Security Center operation and architecture is also assumed, along with a familiarity with system log formats from various operating systems, network devices, and applications and a basic understanding of Linux and Unix command line syntax. For more information, see the [Tenable Security Center User Guide](#).

In addition to the [LCE server](#), Tenable provides the following clients:

- [Tenable Log Correlation Engine Client](#)
- [OPSEC Client](#)
- [Splunk Client](#)
- [Tenable NetFlow Monitor](#)
- [Tenable Network Monitor](#)
- [Tenable RDEP Monitor](#)
- [Tenable SDEE Monitor](#)
- [Web Query Client](#)
- [WMI Monitor Client](#)

Note: While you may still manage clients and policies using an account with Administrator privileges in Tenable Security Center, Log Correlation Engine (versions 4.8 and later) is now the preferred method, as it provides additional validation to client management and policy modification. Additionally, organizations with a centralized instance of Tenable Security Center can better delegate the administration of Log Correlation Engine by utilizing the new features, rather than channeling all Log Correlation Engine administration through Tenable Security Center users with the necessary privileges.

For assistance with Log Correlation Engine, contact Tenable Support.



Get Started

Use the following getting started sequence to configure and maintain your Tenable Log Correlation Engine deployment.

Prepare

- [Components](#)
- [Hardware and Software Requirements](#)

Install

- [Install Tenable Log Correlation Engine Server](#)
- [Run Quick Setup Wizard](#)
- [Offline Configuration & Plugin Updates](#)

Configure

- [Configure Tenable Log Correlation Engine server](#)
 - [Basic](#)
 - [Storage](#)
 - [IDS](#)
 - [Advanced](#)
 - [Control](#)
 - [Feed Setting](#)
- [Files & Layout](#)
- [Configure Organizations](#)

Refine



- [Create, Modify, and Assign Policies](#)
- [Manage Users](#)
- [Manage Clients](#)

Expand

- [Upgrade the Log Correlation Engine Server](#)
- [Upgrade your Log Correlation Engine License](#)
- [Additional Resources](#)



Components of the Tenable Log Correlation Engine

The Tenable Log Correlation Engine (Log Correlation Engine) has three main components:

- The Log Correlation Engine server

The Log Correlation Engine server is a set of cooperating daemons for Red Hat Enterprise Linux (RHEL) or CentOS Linux or Oracle Enterprise Linux (OEL) that collects data from the Log Correlation Engine clients, and then normalizes that data. The normalized data is then analyzed using Tenable Security Center. Tenable Security Center makes both the raw and normalized event data available to the user for event analysis and mitigation. Depending on the scale and requirements of your organization, you may utilize multiple Log Correlation Engine server instances to collect and normalize data.

- The Log Correlation Engine interface

Each Log Correlation Engine server provides a web-based application interface, referred to throughout this documentation as the *Log Correlation Engine interface*. Using the Log Correlation Engine interface, you can monitor the health and status of the Log Correlation Engine server and clients, configure the Log Correlation Engine server, manage clients, create and assign policies, and manage users.

- Log Correlation Engine clients

Log Correlation Engine clients are installed on hosts to monitor and collect events. The event data is then communicated to the Log Correlation Engine server. Events are both stored as raw logs and normalized and correlated with vulnerabilities (if applicable).

Log Correlation Engine users work with log data from a wide variety of sources. Each organization can make queries to one or more Log Correlation Engine servers that process events from devices including firewalls, servers, routers, honeypots, mobile device managers, applications, and many other sources. Log Correlation Engine can collect event data from many sources, including:

- Windows Event Logs (collected locally or remotely via a WMI client)
- Windows, Linux, and Unix system and application logs
- Check Point OPSEC events
- Cisco RDEP events



- Cisco SDEE events
- NetFlow
- Splunk
- Sniffed TCP and UDP network traffic (Tenable Network Monitor)
- Sniffed syslog messages in motion
- Encrypted syslog
- File monitoring for the following operating systems:
 - RHEL
 - Tenable Core
 - FreeBSD
 - Debian
 - OS X
 - AIX
 - Solaris
 - HP-UX
 - Dragon
 - Fedora
 - Ubuntu
 - SuSE
 - Windows
- Salesforce
- Amazon Web Services, via CloudTrail
- Google Cloud Platform

Intrusion Detection and Prevention Systems



Log Correlation Engine has many signature processing libraries to parse logs and can normalize and correlate most network intrusion detection (IDS) and intrusion protection systems (IPS), as well as messages from Tenable Security Center.

Log Correlation Engine supports event collection and vulnerability correlation for the following systems:

- Bro
- Cisco IDS
- Enterasys Dragon
- IBM Proventia (SNMP)
- Juniper NetScreen IDP
- McAfee IntruShield
- Fortinet IDS events
- Snort (and Snort-based products)
- HP TippingPoint

Note: TippingPoint's **syslog** event format must be modified to use a comma delimiter rather than a tab delimiter before it can be processed by Tenable Log Correlation Engine.

Log Correlation Engine supports only event collection for the following systems:

- AirMagnet
- Check Point (Network Flight Recorder)
- Portaledge
- Toplayer IPS

There are thousands of normalization rules that support most operating systems, firewalls, network routers, intrusion detection systems, honeypots, and other network devices. The list of officially supported log sources is frequently updated on the [Tenable website](#).



Hardware and Software Requirements

Before deploying Log Correlation Engine, confirm that the prerequisite software and hardware requirements have been met and that you have an operational instance of Tenable Security Center. Depending on the size of your organization and the way you deploy Log Correlation Engine, the hardware requirements for Log Correlation Engine change. All deployments have a common set of minimum software requirements.

This section contains the following:

- [Software Requirements](#)
- [Hardware Requirements](#)
- [System Specifications](#)
- [Licenses](#)
- [File System Recommendations](#)

Software Requirements

All deployments of Log Correlation Engine require the following:

- An active Log Correlation Engine license
- One of the following operating systems:
 - RHEL/CentOS/OEL 6.x, 64-bit
 - RHEL/CentOS/OEL 7.x, 64-bit
 - RHEL/CentOS/OEL 8.x, 64-bit

Additionally, while Log Correlation Engine is active, it requires exclusive access to certain ports. The only services that are required to support remote users are SSH and the Log Correlation Engine interface (`lce_wwwd`). If other services are active on the system, conflicts should be avoided on the following default ports:

Ports Tenable Log Correlation Engine Receives (Listens) On

Port	Description
------	-------------



162/UDP	SNMP
514/UDP	Syslog
22/TCP	SSH, for requests from Tenable Security Center
601/TCP	Syslog
1243/TCP	Vulnerability detection, if enabled in Tenable Security Center
6514/TCP	Encrypted syslog
8836/TCP	Log Correlation Engine Administrative Web UI
31300/TCP	Events from Log Correlation Engine Clients
5432/TCP	PostgreSQL replication from the master node or the standby node in a high availability configuration. For more information, see High Availability .
7091/TCP	<code>showids</code> commands forwarded from the master node to the standby node in a high availability configuration. For more information, see High Availability .
VRRP	Keepalived virtual IP management in a high availability configuration. For more information, see High Availability .

Ports Tenable Log Correlation Engine Sends On

Port	Description
514/UDP	Syslog (forwarded)
443/TCP	Pull requests to the plugins feed at plugins.nessus.org
601/TCP	Syslog (forwarded)
5432/TCP	PostgreSQL replication to the master node or the standby node in a high availability configuration. For more information, see High Availability .
7091/TCP	<code>showids</code> commands forwarded from the master node to the standby node in a high availability configuration. For more information, see High Availability .
VRRP	Keepalived virtual IP management in a high availability configuration. For more information, see High Availability .



Ports Log Correlation Engine Uses Over Loopback Interface

Port	Description
7091/TCP	Internal communication, showids to lce_queryd
7092/TCP	Internal communication, lce_tasld to lced
7093/TCP	Internal communication, showids to lce_queryd

Caution: The system running the Log Correlation Engine can operate a syslog daemon, but the syslog daemon must not be listening on the same port(s) that the Log Correlation Engine server is listening on.

Hardware Requirements

The hardware requirements for Log Correlation Engine change based on the number of events being processed.

Estimating Events

The following table provides the estimated average number of events from various sources.

Devices	Number of Estimated Events
1 workstation/laptop	0.5 events/sec
1 web-facing app server	20 events/sec
1 web-facing firewall/IDS/IPS	75 events/sec
1 internal application server (low volume)	5 events/sec
1 internal application server (high volume: IIS, Exchange, AD)	20 events/sec
1 internal network device	2 events/sec

To convert your event rate to bytes per day, it is recommended that you multiply your total events/second by 250 bytes/event and multiply by 86,400 seconds/day. For example, assume 100 events per second: 100 events/second * 250 bytes/event * 86,400 seconds/day = 2,160,000,000 bytes/day.



System Specification

The following table specifies the system requirements based on the number of events the Log Correlation Engine server is processing.

Installation scenario	RAM	Processor	Hard disk	Hard disk space
One Log Correlation Engine server with PostgreSQL processing less than 5,000 events per seconds	22 GB	8 cores	10,000 RPM HD, or SSD of equiv. IOPS capability; RAID 0/10 configuration	2.4x Licensed storage size
One Log Correlation Engine server with PostgreSQL processing between 5,000 and 20,000 events per second	30 GB	16 cores	15,000 RPM HD, or SSD of equiv. IOPS capability; RAID 0/10 configuration	
One Log Correlation Engine server with PostgreSQL process greater than 20,000 events per second	58 GB or more	24 cores or more	SSD of IOPS capability at least equiv. to a 15,000 RPM HD; RAID 0/10 configuration	

The Log Correlation Engine server requires a minimum of 20 GB of storage space to continue running and storing logs. The current system disk space is visible on [the Health and Status page](#) of the Log Correlation Engine interface.

To ensure Log Correlation Engine can take full advantage of the host's RAM and CPU resources, Tenable recommends configuring a dedicated swap partition. If the host has N GB of RAM, you will need at least $1.6 \times N$ GB of swap space for best performance.

High Availability Requirements



Tenable strongly recommends using the same system specifications on the master and standby nodes in your high availability configuration, including the following:

- Operating system version, to the patch level
- Layout and size of disk partitions
- File system choice and mount options
- RAM size
- Swap size

For optimal stability and performance, the master and standby nodes should be connected by a fast and reliable network link. For more information about high availability configurations, see [High Availability](#).

File System Recommendations

Placing your activeDb on a networked file system (e.g. NFS) results in inadequate system performance. Tenable recommends that you use EXT3, EXT4, XFS, or ZFS and that you pay close attention to the mount options.

Placing your archiveDb on a networked file system does not impact system performance.

If your file system is:	Tenable recommends:	Tenable does not recommend:
EXT3, EXT4, XFS	noatime	atime or strictatime or relatime or diratime or No *atime at all.
EXT3	barrier=0	barrier=1
EXT4	barrier=0 or nobarrier	barrier=1 or barrier
XFS	nobarrier	barrier
EXT3, EXT4	data=writeback	data=journal or data=ordered or No data=* at all.
ZFS	atime=off	atime=on or relatime=on or No *atime at all.



ZFS	Hardware-dependent	compression=gzip or compression=gzip-N or compression=zle compress=gzip or compress=gzip-N or compress=zle
ZFS	logbias=throughput	logbias=latency or No logbias at all.
ZFS	primarycache=metadata	primarycache=all or primarycache=none or No primarycache=* at all.
ZFS	Hardware-dependent	recordsize=512 or recordsize=1024 or recordsize=2048 or recordsize=4096

Licenses

There is no licensed limit to the number of events or IPs that the Log Correlation Engine can be configured to monitor.

There are different licenses available for Log Correlation Engine based on the total amount of storage used by Log Correlation Engine. The licenses are based on 1 TB, 5 TB, and 10 TB storage sizes. A license for Log Correlation Engine is provided as a part of Tenable Security Center Continuous View. There is no difference in the Log Correlation Engine software that is installed, just the maximum storage size that can be used by Log Correlation Engine. Data that exceeds your license limit will be off-lined.



Install the Log Correlation Engine Server

Before You Begin:

- Download the Log Correlation Engine server package from the [Tenable downloads](#) page.
- Install the software the Log Correlation Engine server is dependent on.

Installation Location

Caution: /opt/lce/ must not contain any symbolic links.

Installing the Package

Note: To ensure consistency of audit record time stamps between the Log Correlation Engine and Tenable Security Center, make sure that the underlying OS makes use of the Network Time Protocol (NTP) as described at http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/sect-Date_and_Time_Configuration-Command_Line_Configuration-Network_Time_Protocol.html

If you are upgrading from a previous version of Log Correlation Engine , please skip this section and see [Upgrade the Tenable Log Correlation Engine Server](#). Please follow the instructions in this section for new installations.

To install the Log Correlation Engine RPM, enter the following command: **rpm -ivh <package name>**, where <package name> is the name of the Log Correlation Engine server package you downloaded from the [Tenable downloads](#) page.

For example:

```
Preparing... #####
[100%]
 1:lce #####
[100%]
The installation process is complete.
Please refer to /var/log/lce_upgrade.log to review installation messages.
```



This is a new installation. To configure LCE, please direct your browser to:
<https://192.168.1.101:8836>

The installation process will create a user and group named *lce* and install the Log Correlation Engine server to the */opt/lce* directory. All files will be installed with the user and group of *lce* except for the majority of Log Correlation Engine daemons, which are set-user-id root. An Log Correlation Engine daemon is started by the root user; once the appropriate port(s) are bound, it will drop root privileges.



Tenable Log Correlation Engine Server Installation

The following procedure must be performed as the root user:

1. [Download the Tenable Log Correlation Engine server package.](#)

Tip: After [downloading the Tenable Log Correlation Engine server package](#), you can view information about the software the server is dependent on by using the following command:

```
# rpm -qRp <LCE rpm>
```

...where <LCE rpm> is the path to and filename of the package you downloaded. For example, /tmp/lce-6.0.2-el6.x86_64.rpm.

2. Confirm the integrity of the package by comparing the MD5 checksum with the one listed in the [product release notes](#).
3. [Install the Tenable Log Correlation Engine server.](#)
4. Copy the activation code from the [Tenable Community site](#), as described in the [Tenable Community Guide](#).
5. Using a web browser, navigate to the address or hostname of the Tenable Log Correlation Engine server on port 8836 (https://<ip or hostname>:8836).

Tip: Ensure that the firewall on the system allows TCP traffic through port 8836, otherwise the web UI will be inaccessible. For example, iptables or firewalls may be blocking port 8836 by default. A full list of required ports is included in the [Software Requirements](#).

6. [Complete the Quick Setup wizard.](#)
7. [Add the Tenable Log Correlation Engine server to Tenable Security Center.](#)



Quick Setup

Before You Begin:

- Complete the [Tenable Log Correlation Engine server installation](#).

Tip: If you need to correct a value during the Quick Setup, you can click the **Previous Step** button.

To complete the quick setup:

1. In a browser, navigate to the Tenable Log Correlation Engine interface for the server (<https://<hostname or IP address>:8836>).

The sign-in page appears.

2. In both the **Username** and **Password** boxes, type *admin*.
3. Click the **Sign In To Continue** button.

The Quick Setup **Change Default Password** dialog box appears.

4. In the **New Password** and **Confirm Password** boxes, type a password that is a minimum of four alphanumeric characters.

Note: Required password complexity can be configured later.

5. Click the **Next Step** button.

The Quick Setup **Proxy Configuration** dialog box appears.

6. (Optional) if a proxy is utilized in the environment where Tenable Log Correlation Engine is deployed, select **Yes**, and then enter the required information into the **Proxy Address**, **Proxy Username**, **Proxy Password**, and **Confirm Proxy Password** boxes.
7. Click the **Next Step** button.

The Quick Setup **Set Activation Code** dialog box appears.

Caution: If the Tenable Log Correlation Engine server instance you are trying to activate is not connected to the Internet, you will need to perform the [Offline Activation procedure](#). Complete that procedure, then continue this procedure from step 9.



8. In a separate browser, find your activation code on the [Tenable Community site](#), as described in the [Tenable Community Guide](#).
9. In the Tenable Log Correlation Engine browser, in the **Activation Code** box, type the corresponding activation code from the Tenable Community site.
10. Click the **Apply** button.
11. Click the **Next Step** button.

The Quick Setup **Port Configuration** dialog box appears.

The boxes are populated with the default ports for each type of communication.

12. (Optional) modify the values, and then click the **Apply** button.

Note: It is recommended that you use the default ports unless a conflict is identified.

13. Click the **Next Step** button.

The Quick Setup **Database Directory** dialog box appears.

By default, the **Database Directory** box is set to `/opt/lce/db/`. The **Database Directory** box specifies the location on the host where the Tenable Log Correlation Engine server will create and maintain silos.

14. Confirm that the available space in the directory is sufficient for your Tenable Log Correlation Engine license.
15. Click the **Next Step** button.

The Quick Setup **Network Ranges** dialog box appears.

16. In the **Monitored Network** box, type the network range that Tenable Log Correlation Engine will monitor. The network range must be entered in either CIDR notation, or `<IP>/<netmask>` format. For example, `192.168.0.0/24` or `192.168.0.0/255.255.255.0`.
17. In the **Excluded Network** box, type a network range that you do not want to be monitored by Tenable Log Correlation Engine. The network range must be entered in either CIDR notation, or `<IP>/<netmask>` format.
18. Click the **Next Step** button.



The Quick Setup **Tenable Vulnerability Management** dialog box appears.

19. (Optional) to send vulnerability reports to Tenable Vulnerability Management, select **Yes**, and then enter the required information into the **Cloud Address**, **Cloud Port**, **Cloud Scanner Key**, and **Scanner Name** boxes.

When the Tenable Log Correlation Engine server is configured to send vulnerability reports to Tenable Vulnerability Management, the Tenable Log Correlation Engine server will query Tenable Vulnerability Management for jobs. The Job Queue Check Rate specifies the amount of time that will elapse between each query.

20. In the **Job Queue Check Rate Min** and **Sec** boxes, specify the amount of time that you want to elapse between each query.
21. Click the **Next Step** button.

The Quick Setup **Complete** dialog box appears.

22. Click the **Restart** button.

Quick Setup is completed, and the Tenable Log Correlation Engine server and services restart. When the restart is complete, you can sign in to the Tenable Log Correlation Engine interface to complete any [additional configuration your organization requires](#), including syslog forwarding, load balancing configuration, and NAT setup for Tenable Log Correlation Engine clients, among other configuration items.



Offline Activation and Plugin Updates

Offline Activation

To activate Log Correlation Engine and update Log Correlation Engine plugins on an air-gapped network:

1. Obtain your Log Correlation Engine activation code from the [Tenable Community site](#), as described in the [Tenable Community Guide](#).
2. Copy the activation code to be used with the offline Log Correlation Engine server.
3. Log in to the offline Log Correlation Engine terminal as the root user.
4. In the CLI in Log Correlation Engine, run the following command:

```
# /opt/lce/daemons/lce_wwwd --challenge
Challenge:
e1e02d38a48603467fb8728b13ada3e29e5e9fd4
Copy the challenge above and paste it (with your Activation Code) into:
https://plugins.nessus.org/v2/offline-lce.php
```

5. Copy the challenge code to be used with the offline Log Correlation Engine server.
6. Go to <https://plugins.nessus.org/v2/offline-lce.php> and enter the activation code and challenge code obtained in the previous steps.
7. Select the generated link to download the current plugin set. Make a copy of the link that is returned. The link provided will be valid until the Log Correlation Engine subscription expires.
8. Save the link, as it will be needed each time the plugins are manually updated.
9. Select the link to download the license key, lce.license, or create an lce.license file by copying the license into a text file from -----BEGIN TENABLE LICENSE----- to -----END TENABLE LICENSE-----.
10. On the Log Correlation Engine server host, copy the lce.license file to /opt/lce/daemons, and run the following command:

```
# /opt/lce/daemons/lce_wwwd --register-offline lce.license
```



11. Go to <https://<ip address of your Ice>:8836> and [complete the Quick Setup](#).
12. To verify the license has been loaded successfully, on the top navigation bar, click **Health and Status**.
13. On the left pane, click **Plugins**.

The **Activation Status** should be *Licensed*.

Offline Plugin Updates

Before you begin:

- Complete step 5 of the [Offline Activation](#) procedure to obtain a link download the latest Ice-combined.tar.gz file.

You will use this link to obtain the latest plugins for the duration of your Log Correlation Engine subscription. The Ice-combined.tar.gz file contains updates for Log Correlation Engine PRM(s), TASL(s), discoveries, client policies, the web client, and the web server.

To perform an offline plugin update:

1. Download the latest Ice-combined.tar.gz file.
2. Log in to the Log Correlation Engine interface (<https://<ip address of your Ice>:8836>).
3. Click **Configuration** on the top navigation bar.

The **Configuration** page appears, displaying the **Basic** section.

4. Click **Feed Settings** on the left pane.

The **Feed Settings** section appears.

5. Under **Offline Plugin Update**, click the **Add Plugins** button, and then select the Ice-combined.tar.gz file you downloaded in step 1.
6. After the file is successfully uploaded, click the **Process Plugins** button. The process may take a short time to complete.
7. To verify the plugins have been successfully loaded, on the top navigation bar, click **Health and Status**, and then, on the left pane, click **Feed**. The **Plugin Set** and the **Plugin Set Loaded**



should now reflect the latest set of plugins. For example, a value of 201907222231 is interpreted as **2019-07-22 22:31**.



Shortcuts for Running SQL Commands and Scripts

For more information about the individual SQL scripts relevant to administration and to troubleshooting or performance tuning, see [Tools](#).

After logging in to a console window and invoking:

```
source /opt/lce/tools/source-for-psql-shortcuts.sh
```

A reminder banner will appear:

```
USAGE of the enabled shortcuts:
```

```
psqlc "<a SQL command>"
```

```
psqlf <path to script with SQL commands> [<arg1> [<arg2> [...]]]
```

```
psqli
```

```
Invokes interactive prompt. Note that you can also invoke SQL scripts  
from within the interactive prompt, like so:  \i <path to script>
```

```
; you will then be prompted for script args.
```

psqlf

You can use the `psqlf` shortcut to run the various SQL scripts packaged with Log Correlation Engine that are found under `/opt/lce/tools/pg-helper-sql/`.

Here is an example of running a SQL script that takes no arguments:

```
psqlf pg-helper-sql/recent-alerts-24hours.sql
```

And here is an example of running a SQL script that takes an argument:

```
psqlf pg-helper-sql/disk-usage-one-silo.sql 0
```

To quickly locate and run a script:



1. Log in to Log Correlation Engine via the command line interface (CLI).
2. Type `psqlf` followed by a space.
3. Type the first few letters of the name of the script you want to run. For example, to run `wal-activity.sql`, you can type `wa`.
4. Press Tab.

`psqlf` automatically completes the name of the script.

5. To run the script, press Enter.

Log Correlation Engine runs the selected script.



SQL Scripts

Caution: You must run `source /opt/lce/tools/source-for-pgsql-shortcuts` once in a console, before you can run `psqlf <someScript.sql>` commands in that console.

File	Usage/Description
Administration: Disk Usage	
<code>activeDb-size.sql</code>	Breaks down datastore's disk usage by major categories.
<code>disk-usage-one-silo.sql</code>	States how much disk is being used by this table and associated database objects. <code><silo#></code>
<code>disk-usage-summary.sql</code>	Gives a concise summary of disk usage by table category (tables which store events, tables which maintain filter pointers, rollup counts tables, etc.) Output of this script has been added to diag report to facilitate troubleshooting.
<code>drop-indexes-on-older-silos.sql</code>	Allows operator to easily free up disk space by dropping indexes on silos which have not yet been archived or trimmed out of activeDb, but are no longer queried. <code>[how old, in whole days, must a silo be to have its indexes dropped]</code>
Administration: PostgreSQL Processes	
<code>breve-processes.sql</code>	Shows the SQL command (up to available screen width) being executed by each process. Automatically refreshes display every N (defaults to 10) seconds. <code>[<refreshInterval_seconds, defaults to 10; 0 to only show once>]</code>



<code>expand-processes.sql</code>	Shows complete SQL command (up to 2048 characters) being executed by each process.
<code>progress-analyze.sql</code>	<p>Lists processes running ANALYZE commands, names the target tables and/or indexes, and estimates progress.</p> <div>[<refreshInterval_seconds, defaults to 15; 0 to only show once>]</div>
<code>progress--bulk-load.sql</code>	<p>Lists processes inserting rows into the siloN tables, and estimates progress; can also track the progress of creating archiveDb snapshots.</p> <div>[<refreshInterval_seconds, defaults to 5; 0 to only show once>]</div>
<code>progress--index-or-reindex.sql</code>	Lists processes running CREATE INDEX or REINDEX commands, names the target objects, and estimates progress.
<code>progress--rebuild-table.sql</code>	Lists processes running CLUSTER commands, names the target objects, and estimates progress.
<code>progress--stream-backup.sql</code>	<p>Lists processes taking a backup (see Perform an Online PostgreSQL Backup) and estimates progress.</p> <div>[<refreshInterval_seconds, defaults to 60; 0 to only show once>]</div>
<code>progress-vacuum.sql</code>	Lists processes running VACUUM commands, names the target objects, and estimates progress.
Administration: Tenable Log Correlation Engine Configuration and Alerts	
<code>alerts-by-day.sql</code>	For more information, see Alerts .



<code>alerts-by-month.sql</code>	For more information, see Alerts .
<code>recent-alerts-24hours.sql</code>	For more information, see Alerts .
<code>show-config--changed-since-rpm-install.sql</code>	<p>Shows the following for each configuration attribute changed since the Tenable Log Correlation Engine RPM was installed:</p> <ul style="list-style-type: none">• Name• Current value• Date of last modification
<code>show-config--mv--event_rules.sql</code>	For clearly displaying the configured event rules. You may find this presentation preferable to the one in Web UI. For more information, see Show All Event Rules .
Administration: License and Utilization Counting Toward License Limits	
<code>show-status.sql</code>	<p>Displays information which had formerly been available in command-line environment by invoking <code>/opt/lce/tools/lce_cfg_utils --display-status:</code> daily syslog counts, syslog sources, Tenable Log Correlation Engine daemons' latest start time, etc. Normally an operator will not need this utility, because all that information is also available in Tenable Log Correlation Engine Web UI.</p>
<code>silos.sql</code>	<p>Lists silos ordered by timestamp of oldest event. For each silo, shows:</p> <ul style="list-style-type: none">• how many events are inside• how much rawlog those events collectively contain• that silo's provenance (whether it had been recorded live, migrated in from an earlier Tenable Log



	<p>Correlation Engine version, or imported from a plain-text file)</p> <ul style="list-style-type: none">• presence in activeDb: N if not, Y if yes, P if present but only temporarily to satisfy “archive-peek” queries.• presence in archiveDb: N if not, Y if yes.• TASL %: what percentage of this silo has been scanned for processing by TASL scripts. <div>[-<N newest silos to show> <N oldest silos to show>]</div>
Statistics About Stored Events and Event Normalization	
<code>dimension-occurrence-stats.sql</code>	<p>Permits insight into distribution of the normalized dimensions (event1, event2, sensor, type, user) among stored events.</p> <p>For additional information, see dimension-occurrence-stats.sql.</p> <div>event1 event2 sensor type user [--long]</div>
<code>ip-occurrence-stats.sql</code>	<p>Reports how many stored events are covered by each configured <code>include_networks</code> range. Also, shows top 100 srcIP by event volume (only including IPs recorded in least 5 events/minute on average): this can help you make a better-informed decisions about what range(s) to configured in <code>include_networks</code>.</p>
<code>normalization-percentages.sql</code>	<p>For each dimension (event1, event2, sensor, type, user) reports for what percentage of stored events the respective dimension is known. The numbers are broken down by silo: this lets you quickly gauge extent of event normalization achieved, as well as track progress over time.</p>



<code>throughput--kilo-eps.sql</code>	<p>Shows volume of event influx, by the hour, in units of 1000 events per second.</p> <p>For additional information, see throughput--kilo-eps.sql.</p> <div><code><daysAgo_max> [<daysAgo_min,default>=0]</code></div>
<code>useful-and-idle--plugins.sql</code>	<p>Helps you make an informed decision about which PRM and TASL plugins can be disabled without decreasing your event normalization levels; lets you immediately identify any custom plugins which are not working.</p> <div><code><silos></code></div> <p>Output subsections:</p> <ul style="list-style-type: none">• Event Counts, by Normalizing .prm File• Non-contributing Plugins, by Containing .prm File• Entirely Non-contributing .prm Files• Entirely Non-contributing .prm Files, Not Already Disabled in Configuration• Event Counts, by Engendering .tasl File• Non-contributing .tasl Files• Non-contributing .tasl Files, Not Already Disabled in Configuration <div>Tip: To disable any of the plugins, run the command provided in the output.</div>
<code>rawlog-storage.sql</code>	<p>Shows percentile statistics for rawlog length in a given silo's events.</p> <div><code><silo> <percent of rows to scan; a whole</code></div>



	<div>divisor of 100></div>
Performance Tuning	
buffer-cache--categories.sql	Summarizes the current allocation of the PostgreSQL buffer cache.
index-usage--silo.sql	For respective tables, shows which indexes have been used in queries and how often.
indexes--nonsilo.sql indexes--silo-fp.sql indexes--silo-proper.sql	Summarizes some useful information about indexes defined on respective tables.
locks.sql	Lists database object locks currently held by user-focused PostgreSQL tasks.
planner-estimates.sql	Shows estimates that the PostgreSQL query optimizer is now relying on when it generates an access plan for querying the given table. For each column, shows <i>M</i> (defaults to 10) most common values. <div><table name> [<mCommonestValues>,,=10]</div>
planner-estimates-silo.sql	For each column, shows <i>M</i> (defaults to 10) most common values. <div><silo#> [<mCommonestValues>,,=10]</div>
routines.sql	Lists stored procedures and gives some rudimentary invocation statistics.
rebuild-rawlog-index.sql	Rebuilds index on the rawlog column. Required to apply modified text search configuration retroactively to events already stored.



	<div><silos></div>
<code>table-access-stats--nonsilo.sql</code> <code>table-access-stats--silo-fp.sql</code> <code>table-access-stats--silo-proper.sql</code>	Shows how many times respective tables had been ANALYZEd and/or VACUUMed, and whether a given table has changed since.
<code>table-sizes-nonsilo.sql</code>	Shows how much disk is being used by each table along with its indexes. <div><table name fragment></div>
<code>top-statements--by--all-exe-time.sql</code>	Tells which SQL commands and stored-procedure calls take the longest to run.
<code>top-statements--by--n-calls.sql</code>	Tells which SQL commands and stored-procedure calls are called most frequently.
Troubleshooting	
<code>identify-currnsilo.sql</code>	Prints numeric ID of the silo that incoming new events are now being written to.
<code>ipfilters-overview.sql</code>	Lists IP filters used in recent queries. Shows the first few IP addresses or IP address ranges of each filter. To see all the IP addresses or IP address ranges belonging to a particular filter, use the <code>reconstitute-ipfilter.sql</code> script.
<code>lock-blockers.sql</code>	Shows which processes are waiting their turn to access a particular database object.
<code>migr-full-status.sql</code>	Details migration plan and how far has each of its items been executed.
<code>n-events--by-hhour--bar-</code>	Displays a rudimentary bar chart to give a rough idea of



<code>chart.sql</code>	<p>variation in log volume through the day or through the week. Another view of this information is provided by the <code>throughput--kilo-eps.sql</code> script.</p> <div><code><silos></code></div>
<code>presence-dim-by-hhour.sql</code>	<p>Displays a concise info-graphic of the presence of a particular type (or user, or sensor, or ...) among the events in a given silo, with half-hourly granularity. This can provide a bare-bones reporting capacity even when a Tenable Security Center connection is interrupted.</p> <div><code><silos> event1 event2 sensor type user <literal></code></div>
<code>recent-kinds-5minutes.sql</code> <code>recent-kinds-60minutes.sql</code>	<p>Summarizes events most recently added to activeDb by kind.</p>
<code>reconstitute-ipfilter.sql</code>	<p>Lists all the IP addresses, or IP address ranges, belonging to a particular filter.</p> <div><code><ipfilterId></code></div>



dimension-occurrence-stats.sql

USAGE: event1|event2|sensor|type|user [--long]

If the `--long` option is not given, only basic information is shown. For example, a partial sample output of `psqlf /opt/lce/tools/pg-helper-sql/dimension-occurrence-stats.sql type` is:

nickn	name	total #	rank by total #	First Seen	Latest Seen
2	network	39,234,655	1	2019 Aug23 15:30	2019 Sep19 18:30
15	database	1,765,733	19	2019 Aug24 16:30	2019 Sep10 19:30
10	restart	1,679,365	20	2019 Aug24 13:00	2019 Sep17 06:30

This table shows that no events of `type=database` have been normalized since Sep 10th. Information such as this can be helpful in troubleshooting PRM issues.

If the `--long` option is given, these additional 5 columns (min, 25th %, median, 75th %, and max) are generated. For example, a partial sample output of `psqlf /opt/lce/tools/pg-helper-sql/dimension-occurrence-stats.sql type --long` would be:

nickn	name	total #	rank by total #	First Seen	Latest Seen	min	25th %	median	75th %	max
2	network	39,234,655	1	2019	2019	0.0073	0.9783	0.9939	0.9987	0.9997



				Aug 23 15: 30	Sep 19 18: 30					
15	datab ase	1,765, 733	19	201 9 Aug 24 16: 30	201 9 Sep 10 19: 30	0.00 93	0.00 94	0.00 94	0.00 94	0.01 02
10	resta rt	1,679, 365	20	201 9 Aug 24 13: 00	201 9 Sep 17 06: 30	0.00 01	0.00 02	0.00 87	0.00 92	0.00 98

The last 5 columns on the right show what fraction of events are normalized with respective dimension. For example, name = network:

- 0.0073 (equivalent to 0.73%) – minimum, also called 0th percentile
- At some point , events constituted fraction of 0.9997 (equivalent to 99.97%) – maximum, also called 100th percentile
- The fraction of 0.9939 (equivalent to 99.39%) has been the median average, also called 50th percentile) The median is a superior way to measure a dataset's average, because it is not as easily skewed by outliers.

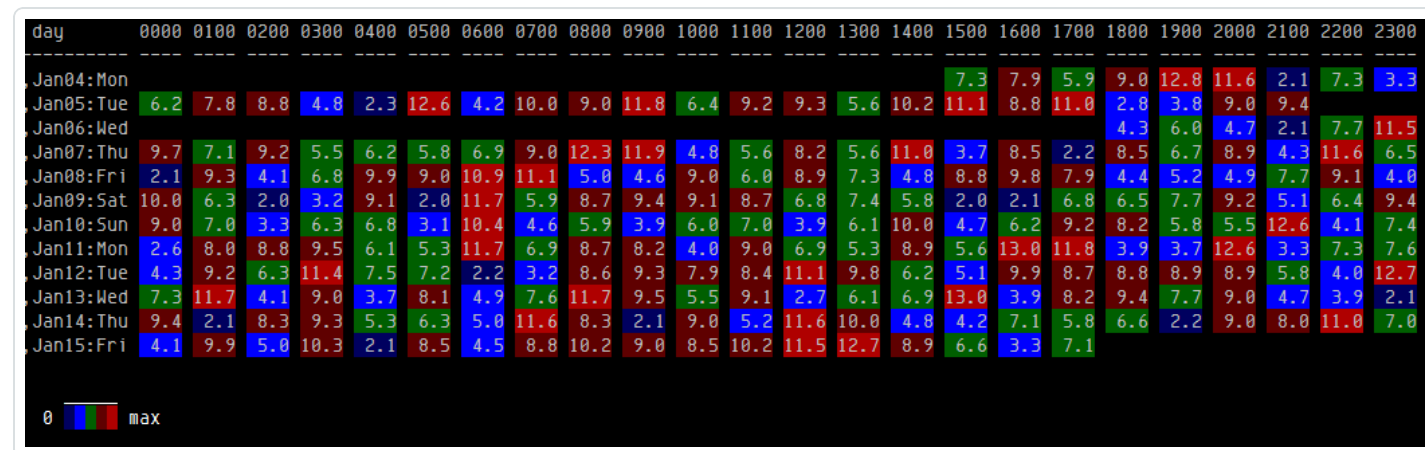


throughput--kilo-eps.sql

```
USAGE: <daysAgo_max> [<daysAgo_min,default>=0]
```

Shows volume of event influx by the hour, in units of 1000 events per second.

Example Output





Files and Layout

Log Correlation Engine resides in the `/opt/lce` directory, and contains various sub-directories. The contents of each subdirectory are summarized in the table below.

Directory	Description
<code>admin/log</code>	<p>This directory contains all of the Log Correlation Engine tracelog files. Tracelogs with expected higher volume are broken up into monthly files, with names in <code>YYYYMon.log</code> format (e.g. <code>2019Jan.log</code>). Tracelog files for some Log Correlation Engine components are stored in eponymous subdirectories.</p> <div>Note: Directory <code>/opt/lce/admin/log</code> is the default location of Log Correlation Engine tracelogs. Use <code>change-tracelogs-location</code> to change the tracelogs directory location. For more information, see change-tracelogs-location.</div>
<code>credentials</code>	<p>This directory contains certificates and keys for Log Correlation Engine modules to authenticate remote connections. For example, the <code>syslog</code> sub-directory contains the default keys and certs to authenticate encrypted TCP syslog senders.</p>
<code>daemons</code>	<p>This directory contains the <code>lced</code> binary (the log engine) and all other helper daemons in Log Correlation Engine. The Log Correlation Engine Client Manager is also located here. The <code>daemons</code> directory also contains sub-directories for plugins, policies, and other items updated automatically via the Log Correlation Engine plugin feed.</p> <p>When Log Correlation Engine starts, it will load all files in the <code>plugins</code> sub-directory unless they are disabled via the configuration.</p> <div>Tip: To verify which version of Log Correlation Engine you are running, run the following command:</div> <div><pre>lced -v</pre></div>
<code>db</code>	<p>Log Correlation Engine stores all event data in the <code>db</code> directory.</p>



Directory	Description
	Note: Directory /opt/lce/db is the default location of Log Correlation Engine activeDb. Use <code>change-activeDb-location</code> to change the activeDb directory location. For more information, see change-activeDb-location .
docs	This directory contains the Log Correlation Engine Software License Agreement.
ids	IDS signature mappings and host vulnerability information from Tenable Security Center is stored here for correlation.
postgresql	Bundled with Log Correlation Engine. For more information, see Location of PostgreSQL Files in an Log Correlation Engine Installation .
reporter	This directory and its sub-directories contain certs and keys for the Nessus Transport Protocol interface for Tenable Security Center to retrieve report information.
reports	This directory contains host vulnerability information Log Correlation Engine has discovered by scanning logs.
tmp	Directory used for temporary data that is utilized by Log Correlation Engine.
tools	This directory contains various tools that are utilized by Tenable Log Correlation Engine , and some can be utilized via the command line if required.
var	The <code>www</code> directory contains the web client, and web server information. The <code>users</code> subdirectory contains a directory for each user configured in the Log Correlation Engine interface.



Location of PostgreSQL Files in an Log Correlation Engine Installation

File	Location	Notes
Data files	<i>tracelogs</i> <i>directory/postgresql</i>	None.
Persistent configuration	<i>tracelogs</i> <i>directory/postgresql</i>	Primary config file is <code>postgresql.conf</code> .
Tracelog	<i>tracelogs</i> <i>directory/postgresql</i>	None. Expect two tracelog files: <code>startup.log</code> and <code>server.log</code> .
Binaries	<code>/opt/lce/postgresql/bin</code>	
Dynamic libraries	<code>/opt/lce/postgresql/lib</code>	To run any of the PostgreSQL binaries (see directly above), your <code>LD_LIBRARY_PATH</code> environment variable must include this directory. The <code>source-for-psql-shortcuts.sh</code> script will do this for you. For more information, see Shortcuts for Running SQL Commands and Scripts .
Setup scripts, timezone rule files, text-search (TS) support files	<code>/opt/lce/postgresql/share</code>	None.



Tenable Security Center CV Integration

Tenable Security Center is used to view events obtained from all of your Log Correlation Engine servers and clients. This section includes:

- [Add Tenable Log Correlation Engine to Tenable Security Center](#)
- [Configure Organizations](#)
- [Analyzing Events](#)
- [Full Text Searches](#)

SSH (Secure Shell) Public Keys

Log Correlation Engine analysis is provided to Tenable Security Center through the use of command execution across a Secure Shell (SSH) network session. When Tenable Security Center queries an Log Correlation Engine server, it invokes an SSH session to the configured Log Correlation Engine server. All execution and analysis of Log Correlation Engine data occurs on the Log Correlation Engine server.

SSH public keys are configured such that Tenable Security Center can invoke commands on the Log Correlation Engine server. Non system-administrator accounts are used to perform these queries. The trust relationship is only needed from Tenable Security Center to the Log Correlation Engine server.



Add Tenable Log Correlation Engine to Tenable Security Center

To add your Tenable Log Correlation Engine server to Tenable Security Center, see [Add a Tenable Log Correlation Engine Server](#) in the [Tenable Security Center User Guide](#).

Option	Description
Name	The unique name that this Tenable Log Correlation Engine server will be known as.
Description	Descriptive text for the Tenable Log Correlation Engine server.
Host	The IP address of the Tenable Log Correlation Engine server. <div>Note: When the Tenable Security Center resides on the same host as the Tenable Log Correlation Engine server, it is recommended to use the localhost IP address of 127.0.0.1.</div>
Organizations	Select the customer that this Tenable Log Correlation Engine is assigned to from the drop down menu.
Event Vulnerability Data	
Import Vulnerabilities	Selecting this box will allow you to configure your Tenable Log Correlation Engine use Event data to detect vulnerabilities.
Repositories	This will allow you to select which repository you would like to keep the vulnerability data collected from Tenable Log Correlation Engine events.
Event Vulnerability Host	
Port	This allows you to configure the port used for communication between Tenable Security Center and Tenable Log Correlation Engine. The default port is 1243. In the Tenable Log Correlation Engine interface this is known as the Reporter Port .
Username	This is the Reporter Username that was set in the Tenable Log Correlation Engine interface under the Configuration, Advanced, Host Discovery and Vulnerabilities section.
Password	This is known as the Reporter Password which is found in the Configuration, Advanced, Host Discovery and Vulnerabilities section.



After clicking on **Submit**, the Tenable Log Correlation Engine admin credentials ("root" user or equivalent) are requested to establish an authenticated session between Tenable Security Center and Tenable Log Correlation Engine. After the Tenable Log Correlation Engine server is successfully added, highlight the new Tenable Log Correlation Engine server to display options pertinent to that server.

Note: If you are using DNS in your environment, make sure it is configured for reverse DNS resolution to facilitate query speeds. If you are not using DNS, modify the /etc/hosts file to include your Tenable Security Center IP address and hostname. For example: 192.0.2.22 SecurityCenter4.example.com
SecurityCenter4



Configure Organizations

Through the web interface, Tenable Security Center can be configured such that users of specific organizations can make queries to each Tenable Log Correlation Engine server. For more information, see [Organizations](#) in the Tenable Security Center User Guide.



Using Tenable Security Center with Tenable Log Correlation Engine

Tenable Security Center is used to visualize data from your Tenable Log Correlation Engine servers. The following section includes:

- [Analyzing Events](#)
- [Full Text Searches](#)
- [Queries Against Archived Snapshots](#)



Analyzing Events

A wide variety of Tenable Log Correlation Engine analysis and reporting tools are available to Tenable Security Center users. These users can make use of any Tenable Log Correlation Engine event that intersects with their range of managed IP addresses. All analysis and reporting options are described in the *Tenable Security Center User Guide*.

Identifying Vulnerabilities

Tenable Log Correlation Engine can leverage log data to find vulnerabilities. The Tenable plugins that report this information will have the plugin ID range of 800,000 - 899,999.

You can filter for the vulnerabilities identified by Tenable Log Correlation Engine in Tenable Security Center by using the "Filters" and selecting "Plugin ID", then selecting "≥" and then entering "800000." The filter setting is pictured below:



Filters <<

Severity ✕
All

Address ✕
All

Vulnerability Text ✕
All

Plugin ID 🗑️
≥ 800000

+ Add More

🗑️ Clear Filters

📄 Load Query

TASL Scripts

After PRM processing normalizes an event, the event is submitted to the Tenable Log Correlation Engine TASL engine for advanced processing by TASL scripts. TASL scripts are used for many types of detection events such as thresholds, successful attack detection, and alerting. By default, all TASL scripts are enabled in the Tenable Log Correlation Engine server; however they can be disabled manually in the “TASL and Plugins” section of the Tenable Log Correlation Engine interface described in detail earlier in this document. For more information regarding TASL scripts review the [Tenable Log Correlation Engine TASL Reference Guide](#).



Full Text Searches

Full text searches may be performed on the data stored within the attached Tenable Log Correlation Engine servers. When viewing the events page the Search field will accept text strings as valid search criteria. Search terms are not case sensitive and a Boolean search may be utilized to further enhance search results. This enables searching the raw logs for details contained in the events.

Tenable Log Correlation Engine can search for compound groups of full text tokens.

Tokens

A token in a full text search is a full word (three or more characters) separated by punctuation or whitespace. For example, if you want to search for logs containing "Microsoft," then Microsoft would be the example of the token.

Operators

Operators are case sensitive, and must be capitalized. For example, a search for *mike* or *miked* will actually yield *mike AND* or *AND miked*. Multiple operators can be used in a single query.

Operator	Description
AND	Finds logs both directly preceding token and the directly following token.
OR	Finds logs containing the directly preceding token, the directly following token, or both.
NOT	Finds logs that do not include the subsequent token.

Wildcards

The * wildcard metacharacter can be used to search for log entries that begin with the token preceding the wildcard in your query. For example, if a wildcard immediately follows a token *T*, then Tenable Log Correlation Engine will match logs containing a token that starts with *T*. So, the query `text='atten*'` will match logs containing "attention," "attenuate," or "Attenborough."

Grouping



Parentheses may be used to group conditionals together to show evaluation precedence just as in mathematics. This is useful in compound conditionals. Without grouping, the query `text='blocked AND denied AND dropped OR firewall'` would return any log with just “firewall” in it because it satisfies the entire query.

The following query would provide a more accurate result: `text='blocked AND denied AND (dropped OR firewall)'`

This requires that the log contains *blocked*, *denied*, and either *dropped* or *firewall*, because it has additional constraints.

Token Adjacency

The relative position of tokens in a log does not normally impact the query results. For example, the query `text='video upload'` will match both “video staging upload success” and “failed to upload video.” If you wish to only match immediately adjacent tokens, surround them with quotation characters “. The query `text='"video upload"'` will not match “video staging upload success” or “failed to upload video,” but it will match “video upload complete.”

If only some of the tokens in your query need to be adjacent, you can surround those tokens with parentheses. For example, if you want to search for logs where “upload” immediately follows “video,” while “studio” can be anywhere, you can query `text='studio ("video upload")'` or `text='("video upload") studio'`.

Token-adjacent search is disabled by default. Enabling token-adjacent search results in a 10% to 15% increase in disk space needed for the database indexes on event log text.

To enable token-adjacent search, run the following command:

```
/opt/lce/tools/cfg-utils --set-sv position_sensitive_text_search true
```

Punctuation

Punctuation characters are normally treated as if they were spaces, separating tokens. The `ts-test` utility, when invoked as `ts-test 'bunnies?possibly!'`, tells us that two `asciiword` tokens are extracted: *bunnies* and *possibly*.

However, if a string looks like a *protocol prefix*, *email address*, *network name*, *URL fragment*, or *file system path*, it will be parsed specially.



For more information about the `ts-test` utility, see [ts-test](#).

Input	Output You May Have Expected	Actual Output
<code>bunnies://</code>	1 token: <i>bunnies</i> , of type <code>asciiword</code>	1 token: <i>bunnies://</i> , of type <code>protocol</code>
<code>mystery.localhost</code>	2 tokens: <i>mystery</i> and <i>localhost</i> , both of type <code>asciiword</code>	1 token: <i>mystery.localhost</i> , of type <code>host</code>
<code>bunnies@mystery.localhost</code>	3 tokens: <i>bunnies</i> and <i>mystery</i> and <i>localhost</i> , all of type <code>asciiword</code>	1 token: <i>bunnies@mystery.localhost</i> , of type <code>email</code>
<code>I forget which chapter/page.Hmm!</code>	4 tokens: <i>forget</i> and <i>chapter</i> and <i>page</i> and <i>hmm</i> , all of type <code>asciiword</code>	2 tokens: <i>forget</i> , of type <code>asciiword</code> ; and <i>chapter/page.hmm</i> , of type <code>file</code>

Search Query Examples:

Query String	What It Means	Example Result	Example Non-Result	Why It Didn't Match
<code>text='Heartbeat'</code>	Show me logs with the term "Heartbeat"	LCE Client Heartbeat 07/23/2014	Heart	does not contain the full term "Heartbeat" by



Query String	What It Means	Example Result	Example Non-Result	Why It Didn't Match
		00:25:00 AM Hostname: Ice_demo IP: 192.0.2.106 Revision: LCE Client 4.2.0 build 20131004		itself, only as a substring
text='linux process'	Show me logs with the term "linux" and the term "process"	This linux host executed process "ls".	This linux host executed nothing.	missing "process"
text='linux NOT process'	Show me logs with the term "linux" but NOT the term "process"	This linux host executed nothing.	This linux host executed process "ls".	contains "process"
text='linux OR nothing'	Show me logs with either term "linux" or term "nothing"	This linux host executed process "ls". This linux host executed nothing.	This nix host did everything.	does not contain "linux" and does not contain "nothing"
text='(linux OR nothing) AND process'	Show me logs that have terms "linux" and "process"	This linux host executed process "ls".	This process did everything.	contains "process" but not "linux" and not "nothing"



Query String	What It Means	Example Result	Example Non-Result	Why It Didn't Match
	or "nothing" and "process"	The process did nothing.	This linux host did nothing.	contains "linux" and "nothing" but not "process"



Queries Against Archived Snapshots

You can query events from a silo in archiveDb if it was archived by Tenable Log Correlation Engine Server 6.0.6 or later. For more information, see [Silo Archiving](#).

Tip: Use the output of `archival-manager --list-snapshots` to determine which Tenable Log Correlation Engine Server version archived the snapshot. For more information about `archival-manager`, see [Tools](#).

When you select a date range in Tenable Security Center using the Archived view, Tenable Log Correlation Engine Server temporarily restores the archived silo into activeDb. This automated process can take several minutes. Therefore, expect a higher than usual latency for the first query against a particular archived silo. Subsequent queries should exhibit normal latency.

Switching between the Active view and Archived view in Tenable Security Center does not remove the archived silo currently occupying the temporary restore slot. For best performance, complete all desired queries against one archived silo before selecting another. For more information about event analysis in Tenable Security Center, see [Event Analysis](#) in the *Tenable Security Center User Guide*.



Health and Status

Included in the Tenable Log Correlation Engine interface is **Health and Status** information. In the **Service Status** section, the name of the service of each daemon is shown along with its status. It also includes when the daemon was last started, and the version of the daemon. The version of the 1ced daemon indicates the version of Tenable Log Correlation Engine you are currently running.

Health and Status Configuration Clients Policies Users

Health and Status

Service Status

Feed

Statistics

Data Sensors

Alerts 1

Advanced


Service	Status	Last Started	Version
Log Engine	Stopped	2019 Jan 09 10:37:53	6.0.0
Query Interface	OK	2019 Jan 09 11:10:19	6.0.0
Vulnerability Reporter	OK	2019 Jan 09 11:10:25	6.0.0
Statistics Engine	OK	2019 Jan 09 11:10:27	6.0.0
TASL Engine	OK	2019 Jan 09 11:10:33	6.0.0
PostgreSQL	OK	2019 Jan 09 10:36:49	11.1






Last Updated: 2019 Jan 9 16:34:00





Feed


The **Feed** section displays the Tenable Log Correlation Engine Server Version, Web Server Version, HTML Client Version, Activation Status, Plugin Set, Plugin Set Loaded, the Feed Expiration information, and the date of the Last Report Uploaded to Cloud.





 Health and Status Configuration Clients Policies Users


 Health and Status

 Service Status


 **Feed**

 Statistics

 Data Sensors

 Alerts

1

 Advanced

Information	Data
Server Version:	6.0.0
Web Server Version:	1.2.5 (Build ID: 20190109)
HTML Client Version:	1.2.5 (Build ID: 20190109)
Activation Status:	Licensed
Plugin Set:	201901041429
Plugin Set Loaded:	201901041429
Feed Expiration:	27 day(s)
Last Report Uploaded to Cloud:	Unknown

Last Updated: 2019 Jan 11 11:33:32



Statistics

In the **Statistics** section the amount of events are displayed by each source of event data. The Tenable Log Correlation Engine source shows the number of internally generated events from the Tenable Log Correlation Engine being administered. The TCP Syslog, and UDP syslog source displays the number of events received on the configured TCP syslog or UDP syslog listening port. Likewise the Clients source is the total amount of event data that all Tenable Log Correlation Engine clients produce. The IDS event source type is the total amount of event data from all IDS sources. The TASL source type is all the event data created by the Tenable Log Correlation Engine TASL scripts.

Health and Status

Configuration

Clients

Policies

Users

Service Status

Feed

Statistics

Data Sensors

Alerts 7

Advanced

Source	Average Events / Second (since startup)	Average Bytes / Second (since startup)	Total Events (today)	Total Events (since startup) ▾
Total	0	0	11	69952
Clients	0	0	0	50429
LCE	0	0	11	9765
TCP Syslog	0	0	0	8167
TASL	0	0	0	1475
UDP Syslog	0	0	0	116
IDS	0	0	0	0

Last Updated: 2018 Jun 29 11:05:50

The source data is displayed in Average Events / Second and Average Bytes / Second since the LCE server was last started. The source data also displays the Total Events (today) for the day, and the Total Events (since startup) is the total number of events since the Tenable Log Correlation Engine server was last started.

Runtime statistics pertaining to logging and correlation are collected, including:

- Logs/bytes per second
- Number/percentage of logs matched/unmatched
- Number of events correlating with vulnerabilities



- Number/percentage of logs from clients, syslog, and IDS
- Number of TASL alerts generated

This information is logged once per hour and is written both to the application log and to the normalized database under the event name **LCE-Server_Statistics** (type "lce").

Example Correlation Statistics Output found in the Tenable Log Correlation Engine admin logs (e.g., /opt/lce/admin/log/2023Jul.log):

```
An average of 50 logs are being received each second.  
A total of 5,778 logs (521,046 bytes) have been received.  
2,232 logs have been matched by plugins (38.63%). 3,546 logs did not match (61.37%).  
Log source breakdown: 5,774 from clients (99.93%), 2 via syslog (0.07%), 0 from IDS  
devices (0.00%).  
No log events have correlated with vulnerabilities.  
2 TASL alerts have been generated.
```



Data Sensors

In the **Data Sensors** section there is a drop-down box, **Select Data Source**, to select the type of data sources to be displayed. The **Clients** option is selected by default, and each client that has sent events to Tenable Log Correlation Engine is displayed. The **Source** column will display the IP address of the client. The **Logs Today** column will show the total number of logs collected by that client in the current day. The **Client Type** column will display the type of client. The **Last Timestamp** column will show when the client last sent an event.

Health and Status Configuration Clients Policies Users

Health and Status

Service Status

Select Data Source:

	Source	Logs Today	Encrypted	Last Timestamp ▾
Feed	127.0.0.1	83	No	2019-02-11 15:02:35

Statistics Last Updated: 2019 Feb 21 12:46:10

Data Sensors

Alerts 720877

Advanced

The second option under **Select Data Source** is **Syslog Sources**, which will display all hosts that are forwarding syslog to the Tenable Log Correlation Engine server. The **Source** column displays the IP address of the syslog server, and the **Logs Today** column displays the total number of logs sent in the last day for each syslog server. The **Encrypted** column shows if the logs being forwarded are encrypted. The **Last Timestamp** column shows the last time each syslog server sent logs to the Tenable Log Correlation Engine server.



Alerts

The **Alerts** section is a simple way to see when a condition on the Tenable Log Correlation Engine server requires attention from the Tenable Log Correlation Engine administrator. It includes informational alerts, such as when a new Tenable Log Correlation Engine client requests authorization to send events to Tenable Log Correlation Engine. It also includes warnings, such as login failures to the Tenable Log Correlation Engine interface, or license expiration warnings. Finally, it includes error conditions that could prevent Tenable Log Correlation Engine from working properly.

Alert Occasions

For every alert created, Tenable Log Correlation Engine Server stores a corresponding *occasion* code, such as `cannot_DNS_resolve`, `client__too_long_inactive`, `license_expired`, or `silo_archival_error`. These codes summarize recent Tenable Log Correlation Engine activity, with help of the following scripts under `/opt/lce/tools/pg-helper-sql`:

File	Description
<code>recent-alerts-24hours.sql</code>	Shows alert counts by occasion grouped by hour for the past 24 hours. Hours without alerts are omitted, and alert occasions with zero occurrences are omitted.
<code>alerts-by-day.sql</code>	Shows alert counts by occasion grouped by day for the past 14 days. Days without alerts are shown, and occasions with zero occurrences are shown. This script can be used for comparing the behavior of multiple Tenable Log Correlation Engine instances monitoring the same Tenable Log Correlation Engine instance over successive weeks.
<code>alerts-by-month.sql</code>	Shows alert counts by occasion grouped by month for the past 12 months.

Example `alerts-by-day.sql` output:









occasion	Sep 09	Sep 10	Sep 11	Sep 12	Sep 13	Sep 14	Sep 15	Sep 16	Sep 17	Sep 18	Sep 19	Sep 20	Sep 21	Sep 22	Sep 23	Sep 24
activeDb_disk_capacity_saturated																
bad_config						4	2	2		3				3	2	
bad_policy																
bad_PRM_plugin																
bad_query																
bad_runtime_state																
bad_saved_control_state																
cannot_DNS_resolve																
cannot_forward_syslog																
cannot_listen_for_clients																
cannot_listen_for_SNMP																
cannot_listen_for_syslog																
client_asked_authorization						7										
client_authorized_explicitly						6		1								
client_error_connecting																
client_error_provisioning																
client_error_receiving																
client_logout_involuntary																
client_too_long_inactive																
events_persist_error																
failover																
license_expired_or_bad																
load_balance_irregularity																
login_acct_administration						1			8							
login_acct_end_session_forced									1							
login_acct_end_session_willed																
login_acct_new_session_allowed																
login_acct_new_session_forbade																
login_acct_session_tokens_mgmt																
migration_irregularity																
misc_alert																
misc_fatal																
plugins_update_done																
plugins_update_irregularity																
reached_license_limit													2			
reached_operating_limit																
silos_archival_error																
silos_create_or_roll_error																
trimming_activeDb																
trimming_archiveDb																
vuln_report_upload_error																





Advanced


The **Advanced** section displays information about the Tenable Log Correlation Engine database. The **Active DB File System Usage** row displays the current amount of disk space being used by the active database, as well as the number of inodes. The **Active DB Oldest Event Time** row displays the timestamp of the earliest event available in the active database. If archiving is enabled, the amount of disk space being used by the archive database and the timestamp of the earliest available event in that database will be included.





 Health and Status Configuration Clients Policies Users


 Health and Status


 Service Status

 Feed

 Statistics

 Data Sensors

 Alerts 1

 Advanced

Silo / Database Metric	Value
Active DB File System Usage	11.40 GB / 49.98 GB (22.81%) and 271,772 inodes / 26,214,400 inodes (1.04%)
Active On Disk Bytes	1.26 KB
Archive DB File System Usage	Archiving Disabled
Estimated Time To Fill Disk	Unknown

Last Updated: 2019 Jan 9 17:07:38



System Configuration

To configure the Tenable Log Correlation Engine server:

1. Log in to Log Correlation Engine via the user interface.
2. On the top navigation bar, click **Configuration**.

The **System Configuration** page appears.

3. Modify your configuration settings. For more information about the sections on the **System Configuration** page, see:
 - [Basic](#)
 - [Storage](#)
 - [IDS](#)
 - [Advanced](#)
 - [Control](#)
 - [Feed Settings](#)
4. Click **Update**.

Log Correlation Engine saves your configuration.

Note: Updates are applied while the Tenable Log Correlation Engine server is operational. You do not need to restart the Tenable Log Correlation Engine services.



Basic Configuration

The Basic Configuration section comprises the essential configuration needed for an Tenable Log Correlation Engine server to function. The items in this section are addressed in the initial Quick Setup, but can be changed in this section at a later time if the need arises.

Each menu option for the **Basic** section is covered in detail below.

Option	Description
Server Address	<p>The IP address of the network interface(s) that the Tenable Log Correlation Engine server listens on. More than one interface may be specified on separate lines:</p> <p>127.0.0.1</p> <p>192.0.2.2</p> <p>By default, or if left blank the above Tenable Log Correlation Engine services will listen on all available network addresses.</p>
Client Port	<p>The port number that the Tenable Log Correlation Engine server listens on. By default, port 31300.</p>
UDP Syslog Port	<p>By default, the Tenable Log Correlation Engine server listens for UDP syslog traffic on port 514. If the environment requires the Tenable Log Correlation Engine server to listen on a different port, this setting may be changed.</p> <div>Note: Only ASCII-encoded syslog is accepted.</div>
TCP Syslog Port	<p>By default, the Tenable Log Correlation Engine server listens for TCP syslog traffic on port 601. If the environment requires the Tenable Log Correlation Engine server to listen on a different port, this setting may be changed.</p> <div>Note: Only ASCII-encoded syslog is accepted.</div>
Encrypted	<p>By default, the Tenable Log Correlation Engine server listens for encrypted</p>



Option	Description
TCP Syslog Listen Port	TCP syslog traffic on port 6514. If the environment requires the Tenable Log Correlation Engine server to listen on a different port, this setting may be changed.
SNMP Port	By default, the Tenable Log Correlation Engine server listens for SNMP traffic on port 162. If the environment requires the Tenable Log Correlation Engine server to listen on a different port, this setting may be changed.
Include Networks	<p>Defines the internal network range. All networks specified in the first section are included.</p> <div><p>Note: Make sure this range matches IP addresses that are considered <i>internal</i> from an event perspective. This range is used by a number of TASL scripts and the stats daemon to define inbound, outbound, and internal specifications for Tenable Log Correlation Engine events. This is different from the Directions filter on the Tenable Security Center events page, which uses the managed ranges of the active user to determine event direction.</p></div>
Exclude Networks	Defines networks that should be excluded from the ranges specified for Include Networks .
Allow only TLSv1.2	Disables all SSL/TLS support prior to TLS 1.2 for all SSL interfaces for PCI DSS compliance.



Storage Configuration

The **Storage** section includes information about the database, including disk space limits for both the active and archive databases.

Health and Status

Configuration

Clients

Policies

Users

System Configuration

Basic

Events Datastore

Storage

IDS

Advanced

Control

Feed Settings

To change the location of the active database, please run:
`/opt/lce/tools/change-activeDb-location path-to-dir`

Database On Disk Space

49.98 GB

Total raw storage capacity of filesystem containing PostgreSQL database.

Active Database Limit

20

TB

Raw storage capacity of the active database, 0 for unlimited

Archived Database Limit

20

TB

Raw storage capacity of the archive database, 0 for unlimited

Archive Directory

/opt/lce/archive/

A directory for oldest data exceeding your license limit or active database limit

Update

Cancel

When your active database reaches the limit you have specified in your configuration, data in that database is moved to the archive database. When the archive limit is exceeded, the oldest archive database is deleted. If you do not want the archive databases to be deleted, set the value for the **Archived Database Limit** option to 0. In that case, storage should be regularly monitored to ensure that enough disk space is available for the active database. If the active database exceeds your license limit, that data will still be archived.

The following table describes the options that are available.

Option	Description
Archiving	

- 70 -



Option	Description
Archive Directory	The directory that stores data that exceeds your license or active database limit.



IDS Configuration

Tenable Log Correlation Engine has the ability to receive IDS events from multiple sources. In addition to being normalized and stored in the log database, each event will be checked against any Tenable Security Center vulnerability databases. If a host is vulnerable to attack, the event is marked as such, allowing rules to trigger on this scenario so that the information can be distributed to the affected administrators.

The screenshot shows the LCE (Log Correlation Engine) interface. The top navigation bar includes 'Health and Status', 'Configuration', 'Clients', 'Policies', and 'Users'. The 'Configuration' section is active, showing 'System Configuration'. On the left, there are tabs for 'Basic', 'Storage', 'IDS', 'Advanced', 'Control', and 'Feed Settings'. The 'IDS' tab is selected, displaying a table of configured sensors. Above the table are input fields for 'Enter IDS IP', 'Enter Sensor Name', and a 'Select Sensor Type' dropdown, along with an 'Add New IDS' button. The table has three columns: 'IDS IP', 'Sensor Name', and 'Sensor Type'. It contains two entries: one with IP 192.168.1.22, name 'Sensor_Bro', and type 'Bro'; and another with IP 192.168.1.66, name 'RealSecure_Sensor', and type 'RealSecure'.

IDS IP	Sensor Name	Sensor Type
192.168.1.22	Sensor_Bro	Bro
192.168.1.66	RealSecure_Sensor	RealSecure

For each IDS sensor, a sensor name and type must be defined as in the example below. The following sensor types are supported:

- Short
- Bro
- RealSecure
- Dragon
- IntruVert
- IntruShield



- Juniper
- NetScreen
- NFR
- Fortinet
- Cisco
- TippingPoint-Sensor
- TippingPoint-SMS

The following table describes the options that are available.

Option	Description
IDS IP	The IP address of the IDS.
Sensor Name	Name to be used within the Tenable Security Center logs.
Sensor Type	IDS sensor type.



High Availability

When high availability is required, Tenable Log Correlation Engine can be configured for two-node replication. A single virtual IP is always bound to the real IP of whichever node is currently the master node. You use the virtual IP in your high availability configuration for all of the following:

- Tenable Log Correlation Engine web UI
- Tenable Log Correlation Engine clients
- Syslog and SMTP inputs
- Tenable Security Center

The two-node high availability configuration allows you to keep log collection and analysis in the event of a hardware or network failure. High availability works by monitoring services on both configured hosts. At any time, the servers in your configuration are assigned either the active (or master) or the standby role. The role of each node is determined by service status, which is monitored at a high frequency. Example timeline:

1. Initial boot
 - Node A initializes in the master role; Node A binds the virtual IP to its primary network interface
 - Node B initializes in the standby role
2. Node A's network connection fails
 - Node B detects Node A's loss of connectivity and takes over the master role
3. Node A's network connection is restored
 - Node A transitions to the standby role
 - Node B maintains the master role
4. Node B's electrical power supply fails
 - Node A takes over the master role
5. Node B's electrical power supply is restored
 - Node B resumes in the standby role



Database synchronization occurs continuously. If a node goes offline and then is restored, ample time is required to re-sync the database. In the event of hardware or network instability that requires the nodes to switch roles more frequently than every 5 minutes, high availability behavior may become unpredictable and may result in missing log data.

Note: If you configure high availability for Tenable Log Correlation Engine, use the virtual IP address when configuring Tenable Log Correlation Engine in Tenable Security Center.

Note: On the standby node, Tenable Log Correlation Engine will run only the following services: `keepalived`, `postgresql`, and `lce_queryd`. Do not manually start, restart, or stop Tenable Log Correlation Engine services on the standby node.

Note: On both the master and the standby node, `ha-manager` will start and stop the `keepalived` service automatically as needed. Do not manually start, restart, or stop the `keepalived` service on either node.

For more information, see:

- [Configure High Availability](#)
- [Monitor Your High Availability Configuration](#)
- [Disable High Availability](#)

Health and Status

You can view status information about your high availability configuration in the LCE web UI or by running `ha-manager --status`.

For more information, see [Monitor Your High Availability Configuration](#).

Migrating Existing High Availability Configurations

If you previously configured high availability on your Log Correlation Engine 4.8.4 deployment and want to migrate to Log Correlation Engine 6.0.4 or later, you can upgrade and then re-configure your high availability configuration, as described in [Migrate Your High Availability Configuration to Log Correlation Engine 6.0.4 or Later](#).

ha-manager Utility

The `ha-manager` utility configures, disables, and provides status details of high availability configurations. For more information about the `ha-manager` utility and its usage, see [ha-manager](#).



Configure High Availability

You can create a high availability configuration by setting up two-node replication with the `ha-manager` utility. If you encounter issues during setup, before restarting the configuration process, use `--disconnect` to disconnect your master and standby nodes without erasing any Log Correlation Engine or PostgreSQL configuration related to high availability.

If you previously configured high availability on your Log Correlation Engine 4.8.4 deployment and want to migrate to Log Correlation Engine 6.0.4 or later, you can upgrade and then re-configure your high availability configuration, as described in [Migrate Your High Availability Configuration to Log Correlation Engine 6.0.4 or Later](#).

For more information about high availability configurations, see [High Availability](#).

Before you begin:

- Confirm the two nodes you intend to use in your high availability configuration have IP addresses in the same broadcast subnet. For example:
 - Standby node 192.0.2.10/24, with non-loopback interface `bond0`
 - Master node 192.0.2.11/24 with non-loopback interface `eth0`
- Consider the following when selecting your virtual IP address:
 - If you are converting a single-node Log Correlation Engine deployment to two-node high availability, use the IP address of your current Tenable Log Correlation Engine server as the virtual IP address and assign a new native IP address to your existing server. This enables Tenable Security Center and Tenable Log Correlation Engine clients to continue operations without reconfiguration.
 - If you are migrating an Log Correlation Engine deployment with high availability configured, use the same virtual IP address you used in your previous configuration.

To configure high availability:

1. At the master node, run:

```
ha-manager --initialize-as-master
```



```
<standby IP address> eth0 <virtual IP address>
```

The `ha-manager` utility initializes setup on the master node.

The `ha-manager` utility prints the estimated size of the *base-backup*, a full copy of the master node's activeDb.

2. At the standby node, run:

```
ha-manager --initialize-as-standby  
<master IP address> bond0 <virtual IP address>
```

The `ha-manager` utility initializes setup on the standby node.

The `ha-manager` utility sends the base-backup of the master node to the standby node.

The `ha-manager` utility prints the `step_2_token`.

The master node prompts you for the `step_2_token`.

Note: The time to complete this step depends on the size of the base-backup. During the transfer, the `ha-manager` utility will print and update the total file size transferred so far.

3. At the master node, type the `step_2_token` and press Enter.

The `ha-manager` utility runs.

The `ha-manager` utility prints the `step_3_token`.

The standby node prompts you for the `step_3_token`.

4. At the standby node, type the `step_3_token` and press Enter.

The `ha-manager` utility runs.

5. When the standby node's `ha-manager` utility finishes running, at the master node, press Enter.

```

bench6 23:54:50 ~/ $ ha-manager --initialize-as-master 172.26.102.47 em3 172.26.102.49

(Reminder: the standby must also have
    broadcast IP=172.26.103.255], activeDb_directory=[/home/bunnies], and tracelogs_dir
    ectory=[/opt/lce/admin/log]
).

===== [ STEP_1: Done ] =====
Size of base-backup to copy = 20G

Now run
    /opt/lce/tools/ha-manager --initialize-as-standby
at the standby host.

Please type in the step_2_token value which will have been printed at standby node:
    788d
===== [ STEP_3: Done ] =====

The step_3_token is a86f; enter that value at the standby node, when asked.

Hit <ENTER> to proceed, once step_4 has completed at standby

===== [ STEP_5: Done ] =====

```

6. When the master node's ha-manager utility finishes running, at the standby node, press Enter.

```

bench7 23:55:01 ~/ $ ha-manager --initialize-as-standby 172.26.102.48 bond0 172.26.102.49

(Reminder: the master must also have
    broadcast IP=172.26.103.255], activeDb_directory=[/home/bunnies], and tracelogs_dir
    ectory=[/opt/lce/admin/log]
).
Size of base-backup copied = 20G

===== [ STEP_2: Done ] =====

The step_2_token is 788d; enter that value at the master node, when asked.

Please type in the step_3_token value which will have been printed at master node:
    a86f
===== [ STEP_4: Done ] =====

Hit <ENTER> to proceed, once step_5 has completed at master

===== [ STEP_6: Done ] =====
bench7 23:59:27 ~/ $

```

7. If only one node has a copy of your SSH keys, run the following command:



```
/opt/lce/tools/ha-manager --copy-SSH-keys-to-peer
```

Log Correlation Engine copies the SSH keys to the peer node.

Note: To ensure both the master node and standby node can respond to requests from Tenable Security Center, both nodes must have the same SSH keys. If both nodes already have a copy of your SSH keys, skip this step.

What to do next:

- Monitor your high availability status, as described in [Monitor Your High Availability Configuration](#).



Migrate Your High Availability Configuration to Log Correlation Engine 6.0.4 or Later

You can use this method to upgrade your Log Correlation Engine 4.8.4 deployment with high availability to Log Correlation Engine 6.0.4 or later, then re-configure high availability. To configure high availability for the first time in Log Correlation Engine 6.0.4 or later, see [Configure High Availability](#). For more information about high availability configurations, see [High Availability](#).

Note: If you are upgrading from a version of Log Correlation Engine earlier than 4.8.4, upgrade to Log Correlation Engine 4.8.4 before upgrading to Log Correlation Engine 6.0.4 or later.

Tip: If you have another node available, you can keep the former standby node offline to use as an emergency backup in case you encounter issues after migration. If you want to keep your former standby node as a backup:

- Skip step three in the procedure below to keep Log Correlation Engine installed on the former standby node.
- Use the third node as the standby node in your new high availability configuration after upgrading to Log Correlation Engine 6.0.4 or later.

To upgrade from Log Correlation Engine 4.8.4 to Log Correlation Engine 6.0.4 or later and re-configure high availability:

1. Log in to Log Correlation Engine via the command line interface (CLI).
2. In the CLI in Log Correlation Engine, run the following commands on both the master node and the standby node to stop Log Correlation Engine :

```
service stats stop
/opt/lce/tools/stop_lce
pkill -KILL keepalived 2>/dev/null
```

Log Correlation Engine stops.

3. (Optional) Make a copy of the master node activeDb.
4. To remove Log Correlation Engine from the standby node, do the following:



- a. In the CLI in Log Correlation Engine, run the following commands:

```
rpm -e lce  
rm -rf /opt/lce/
```

- b. If you configured archiveDb, run the following command:

```
rm -rf <archiveDb directory>
```

- c. If you moved activeDb from the default directory /opt/lce/db/, run the following command:

```
rm -rf <activeDb directory>
```

- d. If you moved tracelogsDir from the default directory /opt/lce/admin/log, run the following command:

```
rm -rf <tracelogsDir directory>
```

5. At the standby node, run the following command:

```
rpm -ivh lce-6.0.4-.....
```

6. At the master node, run the following command:

```
rpm -Uvh lce-6.0.4-.....
```

7. Configure high availability on the master node and the standby node, as described in [Configure High Availability](#).

8. At the master node, run the following command:

```
nohup /opt/lce/tools/migrateDB-overseer --migrate-all --clear-source-on-success &
```

Log Correlation Engine migrates silos to the master node's activeDb and copies them to the standby node's activeDb.

What to do next:



- Monitor your high availability status, as described in [Monitor Your High Availability Configuration](#).



Migrate Your High Availability Configuration to Log Correlation Engine 6.0.5 or Later

You can use this method to upgrade your Log Correlation Engine 6.0.4 deployment with high availability to Log Correlation Engine 6.0.5 or later, then re-configure high availability. To configure high availability for the first time in Log Correlation Engine 6.0.4 or later, see [Configure High Availability](#). For more information about high availability configurations, see [High Availability](#).

To upgrade from Log Correlation Engine 6.0.4 to Log Correlation Engine 6.0.5 or later and re-configure high availability:

1. Log in to Log Correlation Engine via the command line interface (CLI).
2. In the CLI in Log Correlation Engine, run the following command on the standby node to make it a standalone node:

```
/opt/lce/tools/ha-manager --disconnect
```

3. Run the following command on the master node to make it a standalone node:

```
/opt/lce/tools/ha-manager --disconnect
```

4. Run the following commands to remove Log Correlation Engine from the standby node:

a.

```
/opt/lce/tools/stop-all  
rpm -e lce  
rm -rf /opt/lce/
```

- b. If you moved activeDb from the default directory /opt/lce/db/, run the following command:

```
rm -rf <activeDb directory>
```

- c. If you moved traceLogsDir from the default directory /opt/lce/admin/log, run the



following command:

```
rm -rf <tracelongsDir directory>
```

5. (Optional) Backup the activeDb of the master node using `/opt/lce/tools/online-pg-backup`.
6. On the master node, run the following command:

```
rpm -Uvh lce-6.0.x-.....
```

7. On the standby node, run the following command:

```
rpm -ivh lce-6.0.y-.....
```

8. Configure high availability on the master and standby nodes, as described in [Configure High Availability](#).

What to do next:

- Monitor your high availability status, as described in [Monitor Your High Availability Configuration](#).



Monitor Your High Availability Configuration

You can view status information about your high availability configuration in the LCE web UI or by running `ha-manager --status`. For more information about high availability and the `ha-manager` utility, see [High Availability](#).

To view the status of your high availability configuration in the Tenable Log Correlation Engine web UI:

1. In the top navigation bar, click **Health and Status**.

The **Health and Status** page appears.

2. In the left navigation bar, click **Advanced**.

The **Advanced** tab appears.

3. View the following information about your high availability configuration:

- Last HA Replication Ping — the date and time of the last data transmission from the master node to the standby node
- High Availability Status — shows the results of `ha-manager --status`



Silo / Database Metric	Value
Active DB File System Usage	3.03 GB / 57.38 GB (5.28%) and 73,821 inodes / 30,091,264 inodes (0.25%)
Active On Disk Bytes	18.29 MB
Archive DB File System Usage	Archiving Disabled
Last HA Replication Ping	2020-05-05 15:29:58

High Availability Status

pertinent LCE config:

```
failover__peer_physical_IP = 172.26.101.244
failover__virtual_bind_interface = ens192
failover__virtual_IP = 172.26.101.242
queries__percent_forward_to_standby = 60
```

virtual IP: Bound to [ens192]

open and reachable ports:

```
PostgreSQL, this node: listening like a HA-capable node should
lce_queryd, this node: not listening
PostgreSQL, peer node: listening like a HA-capable node should
lce_queryd, peer node: listening like HA standby should
```

commands received during latest run:

```
[May05,20:34:54.833372] --initialize-as-standby 172.26.101.244 ens192 172.26.101.242
[May05,20:35:21.822900] --notify-backup
[May05,20:35:26.629124] --notify-master
```

Keepalived config and status:

PID	%MEM	ELAPSED
7411	0.0	01:13:06
7412	0.0	01:13:06

Advertisements:	VRRP Instance = haLCE
Received: 0	State = MASTER
Sent: 4380	Last transition = 1588725326 (Tue May 5 20:35:26 2020)
Became master: 1	Listening device = ens192
Released master: 0	Using src_ip = 172.26.101.245
Packet Errors:	Virtual Router ID = 164
Length: 0	Priority = 50
TTL: 0	Effective priority = 60
Invalid Type: 0	Preempt = disabled

To view the status of the Keepalived service:



1. In the top navigation bar, click **Health and Status** .

The **Health and Status** page appears.

2. In the left navigation bar, click **Service Status**.

The **Service Status** tab appears.

3. In the **Keep Alive** row, view the current status.

Service	Status	Last Started	Version
Log Engine	OK	2020 May 05 20:35:28	6.0.4
Query Interface	OK	2020 May 05 20:35:28	6.0.4
Vulnerability Reporter	OK	2020 May 05 20:38:09	6.0.4
Statistics Engine	OK	2020 May 05 20:35:34	6.0.4
TASL Engine	OK	2020 May 05 20:35:33	6.0.4
PostgreSQL	OK	2020 May 05 20:35:04	12.1
Keep Alive	OK	2020 May 05 20:35:27	1.3.9



Disable High Availability

For more information about high availability, see [High Availability](#). For more information about the `ha-manager` utility, see [ha-manager](#).

To disable high availability and convert a node into a standalone node:

1. At the node you want to convert into a standalone node, run:

```
ha-manager --disconnect
```

The `ha-manager` utility disconnects the master and standby nodes.

2. Run:

```
ha-manager --de-configure
```

The `ha-manager` utility erases your high availability configuration.



Advanced Configuration

The **Advanced** configuration section is used to fine tune your Tenable Log Correlation Engine server configuration. Each section that is changed in the **Advanced** section will require that the **Update** button is selected before the updates are completed. Select **Cancel** to clear any unwanted updates.

The **Advanced** configuration section includes the following groups of settings:

- [Storage](#)
- [Tenable Log Correlation Engine Web Server](#)
- [Sensor Names](#)
- [Clients](#)
- [User Tracking](#)
- [Host Discovery and Vulnerabilities](#)
- [Statistical Alerts](#)
- [Resource Usage and Performance](#)
- [DNS Caching](#)
- [Data Forwarding](#)
- [TCP Syslog](#)
- [Encrypted TCP Syslog](#)
- [Correlation](#)
- [TASL and Plugins](#)
- [Event Rules](#)

Storage

The options available under the **Storage** subsection are **Store Unnormalized Logs** and **Disk Alert Percentage**. These options are described in the table below.



Option	Description
Store Unnormalized Logs	If enabled, then Tenable Log Correlation Engine will store logs that cannot be normalized by existing Tenable Log Correlation Engine plugins. These logs will have the type and event set to unnormalized and will still be available for text, IP, and sensor-based searches.
Disk Alert Percentage	When filesystem usage exceeds the specified percentage (from 1 to 99 percent), an alert is generated so that you can take action to ensure the Tenable Log Correlation Engine server does not exhaust disk space for log storage. The default value is 75 percent.

Tenable Log Correlation Engine Web Server

The Tenable Log Correlation Engine Web Server section allows you to specify parameters governing login parameters for user access. These options are described in the table below.

Option	Description
Login Banner	Banner to display prior to login, requiring users to positively acknowledge a customized statement or warning. Up to 1300 characters.
Enforce Complex Passwords	Require web server user passwords to have at least 1 uppercase, 1 lowercase, 1 number, and 1 special character.
Min Password Length	Minimum length of a password for a web server user login. This limit only applies to passwords that are created after this option is modified.
Idle Session Timeout	Idle login sessions will be logged out after the amount of time specified in minutes. To disable the timeout, set the value to 0.
Web Server Port	Specifies the port used to access the Tenable Log Correlation Engine interface. By default, port 8836.
Enable SSL for Web Server	When enabled, the engine will require SSL protection for connections to the web server. If this setting is changed, users are disconnected and must log back into the server again.
Enable SSL Client Certificate	If the <code>web_UI_login_client_CA_cert_path</code> configuration attribute is set, the web server will only accept SSL client certificates for user



Option	Description
Authentication	authentication. By default, this option is disabled and the web server allows login only with a username and password.

Sensor Names

This option allows you to override the discovered name of a syslog sensor with a name that is more identifiable in the environment. For example if the host is *syslogserver06.example.com* but that server resides in the research area of the environment, you can set a name that is more identifiable, such as *research_syslog*.

Normally, the sensor name is set to one of the following:

- The source of the log
- The sensor name set on the client itself
- The syslog source
- The plugin that normalizes the log

If you specify a sensor name using the Tenable Log Correlation Engine interface, that name will always be applied to the sensor that corresponds to the IP address. When creating new sensor names, values must be set for both the **Sensor Name** and **IP Address**.

Option	Description
Sensor Name	Sensor name to be used within the Tenable Security Center logs. <div>Note: The sensor name can be a maximum of 128 characters.</div>
IP Address	The IP address of the configured client or syslog source.

Clients

This section of the Advanced Configuration is used to further define how clients are able to connect to the Tenable Log Correlation Engine, and how they are named when viewed in the **Event** section of Tenable Security Center. The configurations are **Public Server Address**, **Auto Authorize Clients**, **Use Client Network Address**, and **Override Sensor Name**, described in the table below.



Option	Description
Public Server Address	<p>If the server is run from behind a device performing Network Address Translation (NAT), and the Tenable Log Correlation Engine clients that the server manages are on the public side of the device, the Public Server Address box must be set to the NAT address so that the managed clients can communicate with the server. The Tenable Log Correlation Engine server will listen for clients based on, in order of preference, the Public Server Address setting, the Server Address setting, or the first IP that it finds Tenable Log Correlation Engine using that is not 127.0.0.1.</p> <div>Caution: When a Public Server Address is specified, all clients on either side of the NAT device must use this address to connect.</div>
Auto Authorize Clients	<p>Specifies the number of minutes after the Tenable Log Correlation Engine server starts that clients will be automatically authorized. For example, if the value is set to 10, any clients that attempt to connect to the server within ten minutes of it starting will be automatically authorized.</p>
Use Client Network Address	<p>Override private client IP in events with the NAT / public network peer IP.</p>
Override Sensor Name	<p>Prefer configured name over discovered name.</p>

The **Client Assignment Rules** section allows for specific policies to be applied to specific client ranges. When a client assignment rule is created, a text box appears in the **Policies** column. In the text box, specify the filenames of the policies that you want applied to clients that fall in the range defined by the rule.

Policies are matched by operating system. If there are multiple policies for a particular operating system, the first applicable policy that is specified for that operating system will be assigned. If none of the specified policies are applicable to a client in the network, the default policy for that operating system will be used.



If **Auto Authorize** is enabled, clients that are discovered in the range defined by the rule will be automatically authorized.

Option	Description
Client Network	A network range in CIDR notation
Auto Authorize	If enabled, clients discovered in the network range are automatically authorized.

User Tracking

Users of the Tenable Log Correlation Engine server are tracked by their username. These options set restrictions on which usernames are considered valid. Any usernames failing to match the specified criteria are disregarded and the user is reported as invalid for the associated log entries.

User Tracking

User Tracking Plugins

5450
1708
7293
3260
3294
3262
3324

Only plugin IDs in this list are used to apply user tracking. Other plugins will normalize usernames, but no tracking is performed based on the source and destination IP addresses. If a username is normalized by these plugins but does not meet the username validity requirements below, it will not be associated with the log and will not be associated with subsequent logs from that IP address.

Accept Letters

☒

If checked, the server will allow usernames to contain letters.

Accept Numbers

☒

If checked, the server will allow usernames to contain numbers.

Valid Username Characters

Other characters that should be considered valid for usernames normalized by the server.

Max Username Length

The maximum number of characters considered valid for usernames normalized by the server.

Untracked Usernames

root
Ice
admin
administrator
Administrator

These users are not tracked. The usernames are normalized and will appear with their associated logs, but no alert is generated when the username switches from one IP to another.

Option	Description
User Tracking	Only Plugin IDs in this list are used to apply user tracking. Other plugins will



Option	Description
Plugins	<p>normalize usernames, but no tracking is performed based on the source and destination IP addresses. Only usernames normalized by these plugins are subject to the additional user tracking restrictions in this section. If a username is normalized by these plugins but does not meet the additional restrictions it will not be associated with the log and will not be associated with the subsequent logs from that IP address. Some IDs of plugins that can be specified for User Tracking Plugins are:</p> <ul style="list-style-type: none">• 4770 (tenable_pvs.prm)• 5450 (mail_imaps.prm)• 1708 (mail_wuimap.prm)• 7293 (os_win2008_sec.prm)• 3260, 3262, 3294 (os_win2k_sec.prm) <div>Note: Tenable Log Correlation Engine login-failure plugins do not normalize usernames because those logs are not assured to provide a valid username, and it would contaminate the username database. Additionally, it is advised never to add a login-failure plugin ID into the list of User Tracking Plugins. Doing so would invalidate user tracking for hosts that triggered the plugin.</div>
Accept Letters	If enabled, the Tenable Log Correlation Engine server will allow usernames to contain letters.
Accept Numbers	If enabled, the Tenable Log Correlation Engine server will allow usernames to contain numbers.
Valid Username Characters	<p>Specifies which special characters are considered valid for usernames. By default, the following characters are considered valid: <code>-_.\$</code>.</p> <p>For example, the following username would be considered valid based on the default value:</p> <p>b.j-smith@a_b.com</p> <div>Note: You cannot specify the semicolon character, <code>;</code> for this option.</div>



Option	Description
Max Username Length	The maximum number of characters considered valid for usernames normalized by the server.
Untracked Usernames	<p>These users are not tracked. The usernames are normalized and will appear with their associated logs, but no alert is generated when the username switches from one IP to another.</p> <p>Example:</p> <ul style="list-style-type: none">• root• Ice• admin• administrator• Administrator• SYSTEM• INTERACTIVE• NETWORKSERVICE• LOCALSERVICE• ANONYMOUSLOGON• Nobody• NTAUTHORITY• DIALUP• NETWORK• BATCH• NO_USER_NAME

Host Discovery and Vulnerabilities



This section defines the parameters used by Tenable Log Correlation Engine to send vulnerability information to Tenable Security Center, as described in the table below.

Option	Description
Enable Host Discovery	This option enables or disables host discovery. When set to yes, new hosts on the network will be discovered and reported based on log data.
Report Interval	The interval, in minutes, in which the report file will be generated and updated on disk. The default is 60 minutes.
Report Lifetime	The lifetime of a report in days. The report will be cleared after this amount of time. The default is 7 days.
Learning Period	This option determines how many days a host has not been seen before an alert will be generated. A setting of at least 1 or 2 days is recommended. After that, any host that was not discovered during the period will be alerted on as new. Without this setting, Tenable Log Correlation Engine will repeatedly discover all of your hosts that are currently running, and not accurately identify hosts that are actually new.
Reporter Port	The port used by Tenable Security Center to retrieve host and vulnerability reports from Tenable Log Correlation Engine.
Reporter Username	The username used by both Tenable Security Center, and Tenable Log Correlation Engine to exchange vulnerability information.
Reporter Password	The password used by Tenable Security Center and Tenable Log Correlation Engine to exchange vulnerability information.
Verify Reporter Password	This field is used for password verification.

Statistical Alerts

Each statistical anomaly is triggered based on a number of deviations. There are multiple Statistical anomalies that can occur on a network. Some examples are Social Network, Login Failure, DNS, Virus, and Database anomalies. The Tenable Log Correlation Engine stats daemon can track these anomalies, and provide feedback when a specific threshold is reached.



Each statistical anomaly is triggered based on a number of deviations. The table below shows what number of standard deviations needs to occur before a statistical anomaly is triggered along with an example event name as it would be seen in the **Events** section of Tenable Security Center.

Type	Minimum number of standard deviations from the mean	Maximum number of standard deviations from the mean	Example
Minor Anomaly	1.0	5.99	Statistics-Login_Minor_Anomaly
Anomaly	6.0	9.99	Statistics-USB_Anomaly
Medium Anomaly	10.0	99.99	Statistics-SPAM_Medium_Anomaly
Large Anomaly	100.00	999999.99	Statistics-Intrusion_Large_Anomaly

Option	Description
Min Standard Deviation	This specifies the minimum standard deviation that must occur for an event before an alert will be generated for it. The higher this number, the more statistically significant a sequence of events needs to be before an alert is raised.
Min Number of Standard Deviations	If an event occurs more or less than 5.0 standard deviation units, an alert will be generated. Setting this value higher will cut down on any sequence of events that occur close to the standard deviation.
Min Statistical History	This specifies the number of iterations (days) per-event are required before alerts will be generated. If a large amount of Tenable Log Correlation Engine data is already present, set this number to a low value or even to zero. The



Option	Description
	stats daemon can be started to read in all or just part of the existing Tenable Log Correlation Engine data. If you have <i>no</i> Tenable Log Correlation Engine data, leave this value around 7 so the stats daemon will not alert on anything until it has 7 days of event data.
Max Occurrence Frequency	If an event occurs more or less than 5.0 standard deviation units, an alert will be generated. Setting this value higher will cut down on any sequence of events that occur close to the standard deviation.
Syslog Alerts	The statistics engine will send anomaly alerts to the syslog servers in this list. It is recommended to include 127.0.0.1 for the local Tenable Log Correlation Engine service.

Resource Usage and Performance

This section of the Tenable Log Correlation Engine **Advanced Configuration** is used to tune the performance of the Tenable Log Correlation Engine server.

Option	Description
Log Processors	<p>This option leverages multicore processors and determines how many threads will be dedicated to log processing.</p> <p>It is recommended that this setting be no higher than the number of CPU cores in the Tenable Log Correlation Engine host system.</p>
Sampleable TASLs	Sampleable TASL scripts may be skipped to alleviate processor load when the TASL queue is full.

DNS Caching

When a log message is defined in a plugin, Tenable Log Correlation Engine provides the option to specify a hostname instead of an IP address for the `srcip` and `dstip` fields. In this case, Tenable Log Correlation Engine automatically attempts to resolve the provided hostname to an IP address



using DNS. Since the same hostname is typically encountered multiple times, caching the results of lookups can greatly increase performance. These options configure DNS caching in Tenable Log Correlation Engine.

A particular hostname or all domain names with a certain extension can be excluded using the **Always Resolve** section. In this case, the matching hosts are looked up at every occurrence. The **Always Resolve** section can be used to maintain a more extensive list of domains to exclude when DNS caching is utilized. The host contained in the **Always Resolve** section of DNS Caching is read when Tenable Log Correlation Engine starts up, but changes to the list can be made at any time. If changes are made to the section the **Update** button at the bottom of the **Advanced Configuration** section of the Tenable Log Correlation Engine interface will need to be selected.

Option	Description
Max Memory for DNS Cache	Tenable Log Correlation Engine will maintain a cache of hostname-to-IP addresses rather than performing the lookup repeatedly, limited to this amount of memory [MB]. The Max Memory for DNS Cache option can go up to 360K domain names.
DNS Cache Period	The DNS Cache Period option specifies the number of days to cache a hostname-to-IP mapping before updating the result with a new lookup. This value can be set between 1 and 30 days.
Always Resolve	If a host ends with an extension listed here, it will be resolved each time it is encountered rather than being cached. List each host or extension on a new line. A particular hostname or all domain names with a certain extension can be excluded using the Always Resolve section. In this case, the matching hosts are looked up at every occurrence. The Always Resolve section can be used to maintain a more extensive list of domains to exclude when DNS caching is utilized. The hosts contained in the Always Resolve section of DNS Caching are read when Tenable Log Correlation Engine starts up, but changes to the list can be made at any time. If changes are made to the section the Update button at the bottom of the Advanced Configuration section of the Tenable Log Correlation Engine interface will need to be selected.
Cache at Startup	Hosts listed in the Cache at Startup are resolved at startup and cached immediately to reduce runtime DNS resolutions and improve performance. The format for these entries is one hostname per line.



Data Forwarding

See [Data Forwarding](#).

TCP Syslog and Encrypted TCP Syslog

See [Receiving Encrypted Syslog](#).

Correlation

Tenable Log Correlation Engine normally matches the vulnerability port with the port given in the normalized event to correlate an event with vulnerability. If this option is disabled, Tenable Log Correlation Engine will ignore this requirement if the vulnerability port is 0, 22, or 445.

Correlation

Port-Restricted IDS
Correlation



To correlate an event with a vulnerability, the engine requires that the vulnerability port and event port match; except for vulnerability ports 0, 22, and 445. If this option is enabled, the engine will always require the ports to match.

TASL and Plugins

See [TASL and Plugins](#).

Event Rules

See [Event Rules](#).



Data Forwarding

Sending Syslog Messages to Other Hosts

The Log Correlation Engine can be the focal point of your entire log aggregation strategy. If a Storage Area Network, `syslog` server, or some other type of log aggregation solution is deployed in your network, the Log Correlation Engine can be configured to send a copy of any received message to one or more `syslog` servers. These messages include any message received from any client.

To configure the Log Correlation Engine to forward these messages:

1. Log in to Log Correlation Engine via the user interface.
2. Click on the **Configuration** section of the Log Correlation Engine interface.
3. Then select **Advanced**, and in that section locate **Data Forwarding**.
4. In the **Syslog Forwarding** section of **Data Forwarding**, enter a line for each `syslog` server.

The actual `syslog` service is not used to forward the messages. All packet generation is handled by the `lced` process.

The format of each entry into the **Syslog Forwarding** section is `IP:port,exclude-header` as shown below. The IP is the address of the `syslog` server to which the messages are sent. The port indicates the UDP port in which the receiving `syslog` server is listening. The **exclude-header** option determines if the Log Correlation Engine appends a custom header to indicate if the messages are sent from the Log Correlation Engine server or not. When omitted or set to `0`, the header is appended. When set to `1`, the header is not added and only the original log message is sent without indication that it was forwarded from the Log Correlation Engine server. If `2` is used the log will be sent in CEF (Common Event Format) format.

The following is an example of the **Syslog Forwarding** section that forwards messages to multiple `syslog` servers utilizing UDP. The first line forwards to UDP port 1234 and appends an Log Correlation Engine server header to each entry. The second forwards to UDP port 514, and an Log Correlation Engine server header is not appended to each entry. The third forwards to UDP port 514 and the log will be sent in CEF format.



Syslog Forwarding

```
192.168.10.50:1234,0
192.168.20.30:514,1
192.168.20.31:514,2
```

The server will forward all events to these UDP servers.
Each line should be:
{IP or hostname}[port,format_flag]
The default port is 514.
The format flag may be:
0 - include server header text
1 - exclude server header text
2 - CEF format, version 0.

The following is an example section of the **TCP Syslog Forwarding** section that forwards messages to multiple `syslog` servers. The first line forwards to TCP port 601 and appends a Log Correlation Engine server header to each entry with an ASCII 10 (Line Feed) delimiter. The second forwards to TCP port 601, and a Log Correlation Engine server header is not appended to each entry. The third forwards to TCP port 1234 and the log will be sent in CEF (Common Event Format) format.

Syslog Forwarding TCP

```
192.168.10.50:601,0,10
192.168.20.30:601,1
192.168.20.31:1234,2
```

The server will forward all events to these TCP servers.
Each line should be:
{IP or hostname}[port,format_flag,ASCII delimiter]
The default port is 601.
The format flag may be:
0 - include server header text
1 - exclude server header text
2 - CEF format, version 0
ASCII delimiter, default LF(ASCII 10)

Log Correlation Engine has the ability to forward logs in CEF format. However, the log is received by Log Correlation Engine whether it is a log message from an Log Correlation Engine Client, Syslog server, IDS or any other compatible log format Log Correlation Engine will convert the original log generated into CEF format. Shown below is a normal syslog message received by an Log Correlation Engine server followed by the forwarded CEF formatted message.

```
Apr 16 11:05:52 jetjaguar sudo:  rongula : TTY=pts/0 ; PWD=/home/rongula ; USER=foo ;
COMMAND=/bin/bash
```

```
CEF:0|Tenable|LCE|4.4.0|1404|Unix-Successful_Sudo|5|dpt=0 dst=192.0.2.23 spt=0
src=192.0.2.66 duser=rongula proto=0 msg=Apr 16 11:05:52 jetjaguar sudo:  rongula :
TTY\=pts/0 ; PWD\=/home/rongula ; USER\=foo ; COMMAND\=/bin/bash
```

Syslog Compliant Messages



Logs forwarded by the Log Correlation Engine will retain the original `syslog` alert level and facility, if one was present. If one was not present, the Log Correlation Engine assigns a log level of **auth.warning**.

Typically, Log Correlation Engine clients do not send `syslog` compliant messages. If a Log Correlation Engine client were configured to monitor a log file that retained an original message's `syslog` alert level and facility, then this would be retained if forwarded by the Log Correlation Engine.

This allows for a remote `syslog` server that is receiving events from the Log Correlation Engine to process the received messages and place them in specific files. Depending on the type of `syslog` server, it may be possible to place logs from a router into one file, operating system logs into another and so on.

Content of Forwarded syslog Messages

When the Log Correlation Engine forwards a message, it also adds any matched information to the log file as shown below if configured to do so:

```
Jun 30 17:45:36 lce: [not-matched] 0.0.0.0:0 -> 192.0.2.1:0 ::  
<37>sshd(pam_unix)[15322]: authentication failure; logname= uid=0 euid=0 tty=NODEVssh  
ruser= rhost=192.0.2.1
```

The “::” characters are used to separate Log Correlation Engine's heading from the original message. In this case, the message would also have been sent with a `syslog` facility/severity of `<37>` since that was the facility of the original message.

Additionally, notice that the Log Correlation Engine tagged the example event above with a `not-matched` keyword. This means that the Log Correlation Engine did not possess a `.prm` file to process the log. If it did, the matched event name would be present in the same location.

If configured to strip the Log Correlation Engine headers from the forwarded `syslog` messages, only the original log message is sent to the remote `syslog` server.

TCP Syslog Server Reconnect Interval

The **TCP Syslog Server Reconnect Interval** sets the interval that the Log Correlation Engine will wait before making a reconnection attempt to the TCP `syslog` server that lost its connection.



TCP Syslog Server Reconnect
Interval

60



Time allowed to pass before the server will attempt to reconnect, if connection to a TCP syslog server is lost.

TCP Syslog

This list of decimal ASCII character codes tells Log Correlation Engine how to delimit TCP syslogs. By default only the standard linefeed character (ASCII decimal 10) is recognized but other products may use special characters.

TCP Syslog

ASCII Delimiters

10

This list of decimal ASCII character codes tells the server how to delimit TCP syslogs. By default only the standard linefeed character (ASCII decimal 10) is recognized. [0-255]



Receiving Encrypted Syslog

Encrypted TCP Syslog

Tenable Log Correlation Engine can be configured to receive encrypted syslog. The configuration to enable this functionality is located in two places. The **Encrypted TCP Syslog Listen Port** can be found by selecting **Configuration** followed by **Basic**, and by default is configured to port 6514. To locate the **Encrypted TCP Syslog** section, select **Configuration** followed by **Advanced**, and scroll down until the **Encrypted TCP Syslog** section is displayed.

The “Encrypted TCP Syslog” functionality requires an rsyslog server configured to send encrypted syslog to the Tenable Log Correlation Engine server. A self-signed certificate can be used, but it is recommended to use a signed certificate from a trusted CA (Certificate Authority). The only configuration requirement in the “Encrypted TCP Syslog” is the “Senders’ CA Cert. PEM-encoded Path”, and the suggested path is `/opt/lce/credentials/syslog/<filename.pem>`.

A fingerprint can be generated, and used for authentication if it is placed in the “Authorized Fingerprints” section of the “Encrypted TCP Syslog” configuration. It is also suggested to include the IP address or DNS name of authorized hosts that will be forwarding encrypted syslog into the “Authorized Hosts” section of “Encrypted TCP Syslog”.

An example configuration is shown below:

Encrypted TCP Syslog

Senders' CA Cert, PEM-encoded Path	<input type="text" value="/opt/lce/credentials/syslog/ca.pem"/>	Path of encrypted syslog senders' CA cert, PEM-encoded
Authorized Fingerprints	<input type="text" value="sha-1:E4:CE:62:19:A2:7F:94:69:8F:FA:C9:B9:0A:40:93:13:FD:CC:D0:ED"/>	Fingerprints (SHA-1 hashes of DER-encoded certificates, per RFC4572) of hosts authorized to send hither encrypted syslog
Authorized Hosts	<input type="text" value="syslog.example.com
192.168.1.101"/>	DNS names or IPs of hosts authorized to send hither encrypted syslog

Option	Description
Senders' CA	Path of encrypted syslog senders' CA cert, PEM-encoded, for validating



Option	Description
Cert PEM-encoded Path	<p>encrypted syslog senders.</p> <p>If this option is used neither an Authorized Fingerprint nor Authorized Host is required.</p>
Authorized Fingerprints	<p>Fingerprints (SHA-1 hashes of DER-encoded certificates, per RFC4572) of hosts authorized to send encrypted syslog. The length of each fingerprint will be 65 characters. This option can be used alone or in conjunction with Authorized Hosts to enable the receipt of TCP Encrypted Syslog.</p> <div>Note: Using an Authorized Fingerprint will only verify the certificate's fingerprint against the configured value. It does not check if the certificate is revoked or expired. It does not require the v3extension.</div>
Authorized Hosts	<p>DNS names or IPs of hosts authorized to send encrypted syslog to the Tenable Log Correlation Engine server. This option can be used alone or in conjunction with Authorized Fingerprints to enable the receipt of TCP Encrypted Syslog.</p> <div>Note: This option is only required if the X509v3 Subject Alternative Name is present in the certificate.</div>



Example Encrypted TCP Syslog Configuration

How the Encrypted TCP syslog is configured depends on the implementation of the rsyslog server that is forwarding the logs to Tenable Log Correlation Engine. For this example, certificates generated by the openssl-utils script contained in the `/opt/lce/tools` directory will be used. The certificates generated by the openssl-utils script are X509v3 certificates that will require the FQDN (fully qualified domain name) of each host. The OS used for this example is CentOS 6 64-bit.

To configure the TCP syslog:

1. Generate CA credentials using `/opt/lce/tools/openssl-utils.sh`.

```
# ./openssl-utils.sh --generate-CA-creds 'C=US,st=MD,CN=lce01.example.com'
/tmp/foo-creds/ca/
```

Generate the certificates for the rsyslog server.

```
# ./openssl-utils.sh --generate-creds devsyslog1.example.com 192.0.2.157
'C=US,st=MD,CN=syslog1.example.com' /tmp/foo-creds/client// /tmp/foo-creds/ca/
```

Generate a client certificate to revoke. This is done to create a certificate revocation list. This is optional.

```
# ./openssl-utils.sh --generate-creds revoke.example.com 192.0.2.47
'C=US,st=MD,CN=revoke.example.com' /tmp/foo-creds/revoked// /tmp/foo-creds/ca/
```

Generate the revocation list certificate. This is only required if you completed the previous step.

```
# ./openssl-utils.sh --revoke /tmp/foo-creds/revoked/cert.pem /tmp/foo-creds/ca/
/tmp/foo-creds/crl.pem
```

2. Copy credentials to `/opt/lce/credentials/syslog`, and to a directory on the remote rsyslog server. Copy the cert.pem certificates to the `/opt/lce/credentials/syslog` directory on your Tenable Log Correlation Engine server.



The certificate will need to be renamed to **rsyslog-ca.pem** so it does not overwrite the Tenable Log Correlation Engine cert.pem file that already exists in the same location.

Caution: Make sure when copying the files to the /opt/lce/credentials directory that you do not overwrite the SSL credentials that were generated at the time of installation. The credentials are **CA-cert.pem**, **CA-privkey.pem**, **server-cert.pem**, and **server-privkey.pem**.

```
[root@test01 ca]# cp /tmp/foo-creds/ca/cert.pem  
/opt/lce/credentials/syslog/rsyslog-ca.pem
```

Copy the certification revocation list (**crl.pem**) to /opt/lce/credentials/syslog directory on your Tenable Log Correlation Engine server.

```
[root@test01 ca]# cp /tmp/foo-creds/crl.pem /opt/lce/credentials/syslog/crl.pem
```

Copy these certificates to a directory on the server running rsyslog. For this example they will be placed in the /root/selfsigned directory of the rsyslog server.

```
/tmp/foo-creds/client/privkey.pem  
/tmp/foo-creds/client/cert.pem  
/tmp/foo-creds/ca/cert.pem
```

Notice that two of these certificates have the same name. It is suggested the certificate from the /tmp/foo-creds/ca/ directory be renamed to **rsyslog-ca.pem**.

3. Set file permissions on the certificates.

Verify the file permissions, and ownership on the certificates that were moved to /opt/lce/credentials/syslog. Each file should be read only by user, and group. They should be owned by Tenable Log Correlation Engine. Use the following commands to change ownership and permissions.

```
# chmod 440 crl.pem  
# chown lce:lce crl.pem  
  
# chmod 440 rsyslog-ca.pem
```



```
# chown lce:lce ca.pem
```

The files moved to the rsyslog server should have the same file permissions, but should be owned by the root user.

```
# chmod 440 rsyslog-ca.pem
# chmod 440 privkey.pem
# chmod 440 cert.pem
```

4. Use your preferred text editor to add the following lines to the rsyslog server configuration (**rsyslog.conf**) file if they are not already present.

```
#$MainMsgQueueType Direct
# set up the action
$DefaultNetstreamDriver gtls # use gtls netstream driver
$ActionSendStreamDriverMode 1 # require TLS for the connection
#$ActionSendStreamDriverAuthMode anon # server is NOT authenticated
$ActionSendStreamDriverAuthMode x509/certvalid

# rsyslog v5 configuration file
# certificate files - just CA for a client
$DefaultNetstreamDriverKeyFile /root/self-signed/privkey.pem
$DefaultNetstreamDriverCertFile /root/self-signed/cert.pem
$DefaultNetstreamDriverCAFile /root/self-signed/rsyslog-ca.pem

# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
*. * @@lce01.example.com:6514
```

Restart the rsyslog service.

```
# service rsyslog restart
```

The following items will need to be included in the Tenable Log Correlation Engine interface configuration of Encrypted TCP Syslog. The path for the Senders' CA Cert, PEM-encoded Path will need to be given, which would be `/opt/lce/credentials/syslog/rsyslog-ca.pem`.



The certificates were generated using X509v3 extensions, which means the FQDN (Fully Qualified Domain Name) will need to be entered into **Authorized Hosts**. After the information has been entered scroll to the bottom of the page, and select **Update**.

5. Configure the “Encrypted TCP Syslog” settings in the Log Correlation Engine interface under **Configuration > Advanced**, and update the configuration.



TASL and Plugins

Excluding TASL Files

TASLs may be disabled selectively by adding the TASL script file name (e.g., `program_accounting.tasl`) to the **Disabled TASL Scripts** section. This option is located under the **TASL and Plugins** portion of the **Advanced** section of the Tenable Log Correlation Engine interface. This is useful for cases where a particular TASL script is not needed by an organization or where the TASL might be causing performance issues and needs to be disabled either temporarily or permanently.

Any disabled TASLs, if removed from the **Disabled TASL Scripts** section, can be re-enabled.

TASL and Plugins

Disabled TASL Scripts

`program_accounting.tasl`

TASL script files listed here will not be loaded or executed. This can be used to increase performance but alerts from these script will not be triggered.

Excluding PRM Files

In some cases, a user may wish to allow the global updates of PRM files, but specifically exclude some from being run. This can be facilitated by using the **Disabled PRM Scripts** section of the Tenable Log Correlation Engine interface. The PRM files to be processed but not loaded can be specified in this location, one per line.

If there is a need to customize a plugin or plugins, rename the original file before making modifications. Once done, include the name of the original plugin in the **Disabled PRM Scripts** section. If an existing PRM file is modified and not renamed, it will be overwritten on the next PRM update. If the original is not disabled, and the Multiple Matches option is not enabled, only one of the two PRM files will match. This option is located under the **TASL and Plugins** portion of the **Advanced** section of the Tenable Log Correlation Engine interface.

Disabled PRM Scripts

`filename.prm`

PRM script files listed here will not be loaded or executed. This can be used to increase performance but logs pertaining to these scripts will not be normalized.



Event Rules

This section is used to configure active response operations used by the Log Correlation Engine daemon. Log Correlation Engine rules are configured to analyze Log Correlation Engine event content and fire if preset conditions are met. Active responses include the ability to send automatic emails (msmtp, sendmail), syslog alerts (syslog, cef), or run custom commands on the Log Correlation Engine system.

Creating Event Rules

To add a new event rule to your configuration, in the **Advanced** section of **Configuration**, under **Event Rules**, click the **Add a New Rule** button. The **Create an event rule window** appears. Using this window, you can specify a name, filters, and an action to be taken.

Create an event rule

Name

Event rule name:

Filters

No filters added.

Filter: Type: Value:

+ Add filter

Source IP (SrcIPs): This filter will search for source IP addresses that are or are not present. The following five formats are supported:

- * 172.16.1.1/255.255.255.0
- * 172.16.1.1/32
- * 172.16.1.1-255
- * 172.16.1.1-172.16.1.255
- * 172.16.1.1

Note that these formats refer to a single value, which can be further delimited with spaces or commas.
Example: 172.16.1.1/32, 192.168.1.1-255, 172.16.10.10

Action

Action: Value:

Shell command (Command): Runs the given command at the command line as user 1ce. A list of replacement macros that allow inserting portions of the original log into the command can be displayed by typing "\$".

Save

Cancel



The following table outlines the syntax that can be applied to filters and actions. [Some examples](#) are also available.

Rule Filters

In the **Filter** drop-down box, select a filter that you want to use for the event rule. The values in the **Type** box are contextual, based on the filter you select. In some cases, you may not need to specify a type. Generally, you will need to specify whether you want to filter data that includes or excludes the values you specify. You can specify multiple filters.

Filters	Description
Source IP (SrcIPS)	<p>This filter will search for source IP addresses that are or are not present. The following five formats are supported:</p> <ul style="list-style-type: none">• 192.0.2.1/255.255.255.0• 192.0.2.1/32• 192.0.2.1-255• 192.0.2.1-192.0.2.255• 192.0.2.1 <p>Each of these formats represent a single value. You can include a comma-delimited list of values using one or a mix of these formats.</p> <p>Example:</p> <p>192.0.2.1/32, 192.0.2.1-255, 192.0.2..10</p>
Destination IP (DstIPS)	<p>This filter will search for destination IP addresses that are or are not present. The following five formats are supported:</p> <ul style="list-style-type: none">• 192.0.2.1/255.255.255.0• 192.0.2.1/32• 192.0.2.1-255• 192.0.2.1-192.0.2.255• 192.0.2.1



Filters	Description
	<p>Each of these formats represent a single value. You can include a comma-delimited list of values using one or a mix of these formats.</p> <p>Example: 192.0.2.1/32, 192.0.2.1-255, 192.0.2..10</p>
IP (IPS)	<p>This filter allows for the search of IP addresses that are or are not present as either source or destination. The following five formats are supported:</p> <ul style="list-style-type: none">• 192.0.2.1/255.255.255.0• 192.0.2.1/32• 192.0.2.1-255• 192.0.2.1-192.0.2.255• 192.0.2.1 <p>Each of these formats represent a single value. You can include a comma-delimited list of values using one or a mix of these formats.</p> <p>Example: 192.0.2.1/32, 192.0.2.1-255, 192.0.2..10</p>
Events	<p>Filter on Log Correlation Engine normalized event name. Considers both the primary and secondary event names.</p> <p>Example: Cisco-IDS_Command_Execution, Windows-Successful_Network_Login, Linux-User_Added</p>
Sensors	<p>Filter on sensor name (available in the Tenable Log Correlation Engine sensor summary view or under Sensor Names) or Tenable Log Correlation Engine client name.</p> <p>Example: XPmarketing01, Win7payroll02</p>
Types	<p>Filter on Log Correlation Engine event type.</p> <p>Example: login, login-failure, intrusion</p>
Ports	<p>Filter on the source or destination port.</p> <p>Example: 80, 443</p>



Filters	Description
Protocols	<p>Filter on the protocol of the event. Note that this means the protocol number as defined by IPv4 (1 for ICMP, 6 for TCP, etc.)</p> <p>Example: 1, 6</p>
Users	<p>Filter on the username in a log.</p> <p>Example: bobt, johnc</p>
Text	<p>Filter on any string in the log (strings can include spaces and punctuation, but not commas).</p> <p>Example: Tenable Network Security</p>
Text, caseless (IText)	<p>Filter on any string in the log, but the text considered would be case insensitive (strings can include spaces and punctuation, but not commas).</p> <p>Example: Tenable Network Security</p>
Vulnerable	<p>Only accepts yes or no. Specify yes if you want to only match logs that correlate to vulnerable hosts.</p>
Threshold	<p>The number of events required over a specified length of time to trigger the rule. The timeframe is expressed using the following format:</p> <p>(integer) in a [second, minute, hour, day, week, month, year]</p> <p>Example: 600 in a minute</p>
MaxQueue	<p>The number of events that will be placed into the event processing queue before being dropped from rule evaluation.</p>
Ratelimit	<p>The maximum number of triggers that will occur over a specified length of time regardless of the number of triggering events. The timeframe is expressed using the following format:</p> <p>(integer) per [second, minute, hour, day, week, month, year]</p> <p>Example: 1 per hour</p>

Rule Actions



In the **Action** drop-down box, specify an action that you want to take based on the filters you created. The following table describes the actions that are available.

Action	Description
Shell command	Runs the given command at the command line as user <code>lce</code> . Examples of the syntax and variables you can use with the shell command follow this table.
Syslog	Forward logs triggered by this rule to the given syslog server. Examples of the syslog syntax follow this table.
CEF	Forward logs triggered by this rule to the given syslog server in CEF format. An example of the CEF syntax follows this table.
Ignore	Causes all events matching the filters to be ignored by Log Correlation Engine. If an event is ignored in this manner there will be no Log Correlation Engine database entry written for it, no other matching event rules will fire, and no TASLs will process this event for alerts. You cannot enter a value for this action.

Email Syntax

Command: **echo "body: \$log" | sendmail rgula@example.com "subject: \$event1 from \$sip"**

Command: **echo "This is a test message." | /opt/lce/tools/msmtp -C /opt/lce/tools/msmtp.conf bob@example.com**

Syslog Syntax

The following syslog line would forward any log that triggered the rule to the remote syslog server 10.10.10.10, port 514, with the default priority of 36 (severity=4, facility=4):

syslog: 10.10.10.10 "Possible password guessing evidence: \$log"

The following syslog line would forward any log that triggered the rule to two remote syslog servers, 10.10.10.9, and 10.10.10.10, on port 515, with the specified priority of 116 (severity=4, facility=14):

syslog: 10.10.10.9, 10.10.10.10 "Your message goes here: \$log" -priority 116 -port 515



CEF Syntax

The following value would forward any log that triggered the rule to two remote syslog servers, 10.10.10.9, and 10.10.10.10, on port 515:

10.10.10.9, 10.10.10.10 -port 515

Custom Command Syntax

Command: **/path/to/scripts/my_custom_firewall_reconfig_command.sh -block \$sip**

Shell Command Variables

The following case sensitive variables may be included in the shell command string. Any commands using one or more the of shell command variables below need to be encapsulated in double quotations ("").

Option	Description
\$sip	Source IP of event
\$dip	Destination IP of event
\$sport	Source port of event
\$dport	Destination port of event
\$proto	Protocol of event, displayed as N/A, TCP, UDP, ICMP, or a number for other protocols
\$vuln	"no" if the event was not correlated with a vulnerability, "yes" otherwise.
\$sensor	Name of sensor generating the event
\$event1	Primary event name
\$event2	Secondary event name
\$type	Type name of event
\$time	Time event was recorded at Log Correlation Engine (format: Mon MM, YYYY H:M:S)



Option	Description
\$user	Username associated with the event
\$log	Raw text of log
\$queued_logs	All logs currently in the event rules queue. Use of this variable has the effect of emptying the rule's queue

Show All Event Rules

You can display all configured event rules ordered by descending time of creation or modification with `psqlf show-config--mv--event_rules.sql`.

Example output:

```
-----+-----
added | val
-----+-----
2020 Dec22 14:58:44 | Save the English knights
                        +SrcIPs: 172.0.0.1
                        -SrcIPs: 8.8.8.8-9.9.9.9
                        Command: /sbin/bunnies/chain-the-attack-rabbit
2020 Oct22 14:53:51 | [Ignore] Cisco - Events (General)
                        +Events: Cisco-Adj_Failed_To_Resolve
                        +Events: Cisco-Line_Down
                        +Events: Cisco-Line_Up
                        +Events: Catalyst-Line_Down
                        +Events: Catalyst-Line_Up
                        +Events: CiscoISE-Radius_Accounting
                        +Events: CiscoASA-Duplicate_TCP_Syn
                        +Events: CiscoASA-Translation_Creation_Failed
                        +Events: CiscoASA-No_Matching_Connection
                        +Events: CiscoASA-Deny_Reverse_Path_Check
                        Ignore
2020 May22 14:55:43 | [Alert] Paloalto-System_Critical_Msg
                        +Events: Paloalto-System_Critical_Msg
                        Command: printf "Subject: [Alert] [Alert] Paloal
to-System_Critical_Msg Palo Alto - Critical System Message\n\nTime: \nSensor: \nType: \nUser:
\nVulnerability: \nEvent Details:\n\n\n\nLog:\n" | /opt/lce/tools/msmtp -C /opt/lce/tools/ms
mtp.conf Joe.Q.Customer@someplace.com
```



Event Rules Examples

Log Correlation Engine can be configured with the ability to interpret received log events based on log content and use configurable rules to generate active responses from the Log Correlation Engine server. These rules are configured in the Log Correlation Engine interface in the **Event Rules** section and can perform three primary responses:

- email alerting
- syslog alerting
- command execution

Note: The Log Correlation Engine server will generate email alerts using the settings found in `msmtp.conf` file, which can be found in the `/opt/lce/tools/` directory on the Log Correlation Engine server. This file will need to include your email server information for alerting to function correctly.

Example: Sample msmtp.conf File

```
# Example msmtp configuration file
#
# Please replace the following with the desired settings for mail server, encryption
and authentication. The full
# msmtp documentation is located at http://msmtp.sourceforge.net/doc/msmtp.html.
#
# msmtp usage example: echo "This is a test message." | /opt/lce/tools/msmtp -C
/opt/lce/tools/msmtp.conf your_name@your_address.com
account provider
host smtp.gmail.com
tls on
tls_certcheck off
tls_starttls off
from your_username@your_domain.com
auth on
user your_username
password your_password
port 465
logfile /opt/lce/tools/msmtp.log
# Set the above account to be the default when the -a flag is not used
account default : provider
```



Examples of practical applications include configuring rules to rate limit certain types of log events, email administrators immediately when an attack is detected, and send customized commands to a firewall when an inbound attack is detected and firewall reconfiguration needs to take place.

Various fields within the received log alert are automatically placed in variables that may be used as parameters within the active response. For example, consider the following **Event Rules** entry:

```
Name: DMZ Login
+IPS: 192.168.20.15,192.168.20.100,192.168.20.110-112
Event: SC4-Login
Command: echo "body: $log" | sendmail rgula@example.com "subject: $event1 from $sip"
RateLimit: 5m
```

This rule takes Log Correlation Engine events labeled "SC4-Login" to the specified IP addresses and automatically generates an email alert to the specified administrator email addresses. In addition, a rate limit is applied such that only one email would be sent every five minutes to prevent the Log Correlation Engine server from overwhelming the email server system. Configuration possibilities are limited only by the imagination of the Log Correlation Engine server administrator.



Service Control

The **Control** section of **System Configuration** is used to verify the status of an Tenable Log Correlation Engine service. This section can also be used to start and stop each service that is related to Tenable Log Correlation Engine if needed.

Option	Description
All Processes	Stop or Start all Tenable Log Correlation Engine daemons
Log Engine	Stop or Start the Tenable Log Correlation Engine daemon
Query Interface	Stop or Start the Tenable Log Correlation Engine query daemon
Vulnerability Reporter	Stop or Start the Tenable Log Correlation Engine Vulnerability Reporter daemon
Statistics Engine	Stop or Start the Statistics daemon
TASL Engine	Stop or Start the TASL Engine daemon.



Feed Settings

The Feed Settings section contains the following groups of settings:

- [Feed Registration](#)
- [Plugin Update](#)
- [Offline Plugin Update](#)
- [Web Proxy](#)
- [Tenable Vulnerability Management Configuration](#)



Feed Registration

The **Feed Registration** section is where the activation code is entered. Once a new code is entered, click the **Apply** button.

Feed Registration

Activation Code

ZD-LCE-1FFE-20BA-3DA1-4F4F-50A

Apply

Option	Description
Activation Code	Your activation code is obtained from the Tenable Community site , as described in the Tenable Community Guide . If a new code is required, type it in the field and click the Apply button.



Plugin Update

Updating Plugins (PRM Files) and TASL Scripts

This section describes the method for updating Tenable Log Correlation Engine plugins (files with a .prm extension) and TASL scripts. Plugin updates occur over a HTTPS connection at a set interval. The default update interval is set to 3 days, but can be increased or reduced if required. The Tenable Log Correlation Engine interface **Plugin Update** section, which is found in the **Configuration** section under **Feed Settings**, can be easily used to update all plugins along by clicking the **Update Plugins** button.

The directories containing the PRM files and TASL scripts are specified in the `/opt/lce/daemons/plugins` directory. When you update plugins, the files contained in the `/opt/lce/daemons/plugins` directory, which are plugins and correlation scripts (TASL) will be archived to the `/opt/lce/daemons/plugins_archive` directory. The backups of the files in the TASL directory will appear in the `plugins_archive` directory as a file such as `tasls.tar.gz`, and the backups of the files in the plugins directory will appear in the `plugins_archive` directory as a file such as `lce.tar.gz`. The backup is only kept until the next plugin update.

Offline Updates

The **Offline Plugin Update** section can be found in the **Configuration** section of the Tenable Log Correlation Engine interface under **Feed Settings**. It allows for a .tar file of the Tenable Log Correlation Engine plugins to be uploaded by browsing to the file, and then clicking the **Process Plugins** button.

Option	Description
Offline Update File	Used to upload a new set of plugins to the Tenable Log Correlation Engine. This is only required if an Tenable Log Correlation Engine server does not have internet access.
Process Update	Clicking this button will complete the update process using the plugins file that was uploaded.



Web Proxy

Option	Description
Proxy Address	The IP address of the proxy server to be used with Tenable Log Correlation Engine
Proxy Username	The username for the proxy if it is required
Proxy Password	The password for the proxy if its required
Verify Proxy Password	The password entered again for verification
Custom Plugin Feed Host	If a custom plugin feed is used with the Tenable Log Correlation Engine server, that host information is entered here.
Custom User Agent	Custom user agent string used during plugin update requests.



Tenable Vulnerability Management Configuration

Option	Description
Cloud Address	The IPv4 address or hostname of Tenable Vulnerability Management, usually cloud.tenable.com.
Cloud Port	[1-65535] Usually 443
Cloud Scanner Key	User-specified key to connect to Tenable Vulnerability Management.
Scanner Name	User-specified Tenable Log Correlation Engine scanner name when connects to Tenable Vulnerability Management. <div>Note: The scanner name can be a maximum of 128 characters.</div>
Job Queue Check Rate	A value between 5 seconds and 60 minutes. By default, 15 seconds



Refresh or Replace the Vulnerability Reporter SSL Certificate

Required User Role: Administrator

To update the self-signed SSL certificate used to upload vulnerability reports to Tenable Security Center, do one of the following:

- Rotate the self-signed SSL certificate, replacing it with a fresh self-signed certificate.
- Replace the self-signed SSL certificate packaged with Log Correlation Engine with an SSL certificate from your organization.

To rotate the self-signed SSL certificate and replace it with a fresh self-signed certificate:

1. Log in to Log Correlation Engine via the command line interface (CLI).
2. In the CLI in Log Correlation Engine, run the following command to refresh the SSL certificate:

```
/opt/lce/tools/lce_crypto_utils --generate-creds-vulnReporter -q
```

Log Correlation Engine regenerates the SSL certificate locally.

3. Re-add the Log Correlation Engine to Tenable Security Center, as described in [Add a Tenable Log Correlation Engine Server](#) in the *Tenable Security Center User Guide*.

To replace the SSL certificate used to upload vulnerability reports to Tenable Security Center:

1. Copy the following files from your CA to `/opt/lce/reporter/ssl/`.
 - cacert.pem
 - servercert.pem
 - cakey.pem
 - serverkey.pem

Note: Do not change the certificate file names.



2. Add the Log Correlation Engine to Tenable Security Center, as described in [Add a Tenable Log Correlation Engine Server](#) in the *Tenable Security Center User Guide*.



Upgrade the Log Correlation Engine Server

Required User Role: Root user

For information about new features, resolved issues, third-party product updates, and supported upgrade paths, see the [release notes](#) for Log Correlation Engine.

Note: All Log Correlation Engine server installations are compatible with Client versions 4.0.0 and later. Older Log Correlation Engine clients will not be able to log in and send event data to Log Correlation Engine 4.4 - 5.1.

Before You Begin

- Download the Log Correlation Engine server package from the [Tenable Downloads](#) page.

Note: The complete PostgreSQL 11.1 is bundled inside the Log Correlation Engine RPM.

To upgrade the Log Correlation Engine server:

1. Log in to Log Correlation Engine via the command line interface (CLI).
2. In the CLI in Log Correlation Engine, run the following command, where *<package name>* is the name of the Log Correlation Engine server package you downloaded from the Tenable Downloads page:

```
rpm -Uvh <package name>
```

The upgrade begins.

```
# rpm -Uvh lce-6.0.0-el6.x86_64.rpm
Preparing... #####
[100%]
1:lce warning: /opt/lce/.ssh/authorized_keys
created as /opt/lce/.ssh/authorized_keys.rpmnew
##### [100%]
The installation process is complete.
Please refer to /var/log/lce_upgrade.log to review installation messages.
```



To configure Tenable Log Correlation Engine, please direct your browser to:
<https://192.168.0.123:8836>

3. (Optional) Migrate your silos using the `/opt/lce/tools/migrateDB-overseer` utility. The utility supports the following operations:

Operation	Description
<code>--estimate-required-disk-space</code>	Estimates how much disk space your 5X silos will need, once migrated into 6X datastore; note, this estimate does not account for events created "live" by Tenable Log Correlation Engine in the course of its normal operation while migration is running. If needed it will remind you to give the <code>--clear-source-on-success</code> option to <code>--migrate-all</code> operation.
<code>--estimate-total-duration</code>	Shows conservative estimates for how long the migration will take for each plausible <code>nParallelWorkers</code> value. Also shows what <code>nParallelWorkers</code> value will be chosen by default.
<code>--migrate-all [--clear-source-on-success] [<nondefault_nParallelWorkers>]</code>	<p>If you do not specify <code>--clear-source-on-success</code>, the Tenable Log Correlation Engine 5X silos will be left as they were, after Tenable Log Correlation Engine 6.0.0 silos with the same contents are built. This could lead to running out of disk space.</p> <div>Note: While a higher value means a faster migration, it also means less resources will remain for normal Tenable Log Correlation Engine operation.</div>
<code>--status</code>	Use this option at any time, from another shell console, to see how migration is progressing.

Caution: Prior to beginning an event silo migration, you should take precautions to ensure there will be sufficient disk space. A silo in the Tenable Log Correlation Engine 6.0.x PostgreSQL format will



require more disk space than the same silo in the Tenable Log Correlation Engine 5.x Elasticsearch format.

Note: Tenable *strongly* recommends running the `/opt/lce/tools/migrateDB-overseer --migrate-all` command instead of migrating one silo at a time with `--migrate-one`. With the `--migrate-all` option, the silos with the most recent events will be migrated first, followed by older silos. With `--migrate-one`, you cannot automatically undo in event of failure. Using `--migrate-one` does not guard against event loss or progress bookmarking for correct resumption after premature termination.

Note: If your SSH console session times out after you start `migrateDB-overseer`, the migration will stop (and you need to start it again later). To avoid this issue, start `migrateDB-overseer` in console-detached mode:

```
nohup /opt/lce/tools/migrateDB-overseer &
```

or

```
nohup /opt/lce/tools/migrateDB-overseer --migrate-all --clear-source-on-success  
&
```



Upgrade your Log Correlation Engine License

You can upgrade your Log Correlation Engine license to a license with higher capacity (e.g., 1 TB to 10 TB). Upgrading your Log Correlation Engine license requires a new license key.

To upgrade your Log Correlation Engine license:

1. Log in to the Log Correlation Engine interface.
2. In the top navigation bar, click **Configuration**.

The **Configuration** page appears, displaying the **Basic** section.

3. In the left navigation bar, click **Feed Settings**.

The **Feed Settings** section appears.

4. In the **Activation Code** box, type your new activation code, and then click the **Apply** button.
5. At the bottom of the **Feed Settings** section, click the **Update** button.

Log Correlation Engine applies the new license.

Tip: To confirm the license upgraded successfully, navigate to **Health and Status**, and select **Plugins** to verify the **Activation status** is *Licensed* and the **Feed Expiration** does not show *Expired*.




Users


The Tenable Log Correlation Engine interface can be accessed by two user types: **Administrator** and **Read Only**. An **Administrator** user has the ability to perform all administration of the Tenable Log Correlation Engine interface. The **Read Only** user can only view the **Health and Status** page. A user's privilege can be seen under **User Type**.


Note: Generally, when this documentation refers to a user, it means a user with Administrator privileges. Otherwise, the documentation will specify a *Read Only* user.


For more information, see:


- [Add Users](#)
- [Edit Users](#)
- [Delete Users](#)
- [Change a User's Password](#)
- [Lock a User Account](#)
- [Unlock a User Account](#)
- [View User Accounts](#)
- [Certificate-Authenticated Web UI Logins](#)


LCE 


 Health and Status

 Configuration

 Clients

 Policies

 Users

 Users

<input type="checkbox"/>	Name ▲	Last Login	Status	User Type
<input type="checkbox"/>	admin	January 14, 2019 11:45:36	Ok	Administrator

Locked User Accounts

Users with locked accounts cannot login until an administrator unlocks their account. User accounts may be automatically locked if they do not follow the password reuse or login session policies an administrator configured. For more information about site policies, see [Site Policies](#).



If a user's account becomes locked while that user is logged in, Tenable Log Correlation Engine immediately terminates the locked user's session.

You can unlock a user's account by doing one of the following:

- Resetting their password, as described in [Change a User's Password](#).
- Using the `user-utils` utility, as described in [Unlock a User Account](#).

You can check to see if a user's account is locked via the Tenable Log Correlation Engine web UI or the CLI, as described in [View User Accounts](#). To lock a user's account, see [Lock a User Account](#).



Add Users

For more information, see [Users](#).

To add a new user:

1. Log in to Log Correlation Engine via the user interface.
2. In the top navigation bar, click **Users**.

The **Users** page appears.

3. Click **+New User**.

The **+New User** window appears.

4. In the **Username** box, type a username that meets the following criteria:
 - Uses only ASCII alphanumeric characters, at signs, periods, underscores, or hyphens
 - Begins with an alphanumeric character or an underscore
 - Does not contain multiple consecutive periods, underscores, or hyphens
 - Uses fewer than 127 characters
5. In the **Password** box, type a temporary password for the user.
6. In the **Confirm Password** box, type the temporary password again.
7. (Optional) To make this user an administrator, select the **Administrator** check box.
8. Click **Create User**.

Log Correlation Engine saves your configuration.



View User Accounts

Required User Role: Administrator

For more information, see [Users](#).

To view a list of users via the Tenable Log Correlation Engine web UI:

1. Log in to Log Correlation Engine via the user interface.
2. In the top navigation bar, click **Users**.

The **Users** page appears.

3. View details about each user account:
 - **Name** — The username for the user.
 - **Last Login** — The date and time the user last logged in to Tenable Log Correlation Engine.
 - **Status** — The status of the user's account.

Status	Description
Ok	The user's account is working normally.
Locked	The user cannot log in to Tenable Log Correlation Engine. To allow this user to log in to Tenable Log Correlation Engine, unlock their account, as described in Unlock a User Account .

- **User Type** — The user's role: **Administrator** or **Read Only**.

To view a list of user accounts via the CLI:

1. In the command line interface (CLI), run the following command:

```
/opt/lce/tools/user-utils --list-all
```

The `user-utils` utility prints a table of users with the following details:



- **Purpose** – The user's role.
- **Note:** In the printed table, **Administrators** are labeled **WebUI admin** and **Read Only** users are labeled **WebUI readonly**.
- **Username** – The user's username.
- **Locked acct?** – Indicates whether the user's account is locked (**yes** or **no**). For more information, see [Locked User Accounts](#).
- **Temp. passw?** – Indicates whether the user has a temporary password (**yes** or **no**).
- **Last Reset** – The date and time of the user's most recent password reset.
- **Last Auth Success** – The date and time of the user's most recent login.
- **Last Activity** – The date and time the user interacted with the Tenable Log Correlation Engine web UI.



Edit Users

For more information, see [Users](#).

Note: After you set a temporary password for a user, the user must change their password the next time they log in to LCE.

To edit a user via the Tenable Log Correlation Engine web UI:

1. Log in to Log Correlation Engine via the user interface.
2. In the top navigation bar, click **Users**.

The **Users** page appears.

3. Click the row for the user.

The **Edit User** window appears.

4. Modify the user details.
5. Click **Update**.

Log Correlation Engine saves your configuration.

To edit a user via the CLI:

- To lock a user's account, run:

```
user-utils --lock--WebUI-acct <username>
```

- To unlock a user's account, run:

```
user-utils --unlock--WebUI-acct <username>
```

- To change a user's password, run:

```
user-utils --set-password--WebUI-acct <username>
```



Change a User's Password

Required User Role: Administrator

For more information, see [Users](#).

Note: After you set a temporary password for a user, the user must change their password the next time they log in to LCE.

To change a user's password via the Tenable Log Correlation Engine web UI:

1. Log in to Log Correlation Engine via the user interface.
2. In the top navigation bar, click **Users**.

The **Users** page appears.

3. Click the row for the user.

The **Edit User** window appears.

4. In the **New Password** field, type a temporary password for the user.
5. In the **Confirm Password** field, type the temporary password again.
6. Click **Update**.

Log Correlation Engine saves your configuration.

To change a user's password via the CLI:

1. Log in to Log Correlation Engine via the command line interface (CLI).
2. In the CLI in Log Correlation Engine, run the following command:

```
user-utils --set-password--WebUI-acct <username>
```

The `user-utils` utility prompts you for a temporary password.

3. Type a temporary password for the user and press Enter.

The `user-utils` utility sets the temporary password for the user.



Delete Users

For more information, see [Users](#).

To delete a single user:

1. Log in to Log Correlation Engine via the user interface.
2. In the top navigation bar, click **Users**.

The **Users** page appears.

3. In the row for the user you want to delete, click **x**.

The **Delete User** window appears.

4. Click **Delete**.

Tenable Log Correlation Engine deletes the user account and immediately terminates the deleted user's session.

To delete multiple users at once:

1. Log in to Log Correlation Engine via the user interface.
2. In the top navigation bar, click **Users**.

The **Users** page appears.

3. In the row for each user you want to delete, select the check box.
4. In the **Actions** drop-down box, click **Delete Users**.

The **Delete User** window appears.

5. Click **Delete**.

Tenable Log Correlation Engine deletes the user accounts and immediately terminates the deleted users' sessions.



Unlock a User Account

Required User Role: Administrator

Users with locked accounts cannot login until an administrator unlocks their account. User accounts may be automatically locked if they do not follow the password reuse or login session policies an administrator configured. For more information about site policies, see [Site Policies](#).

For more information about user accounts, see [Users](#).

Tip: Resetting a locked user's password unlocks their account. For more information, see [Change a User's Password](#).

Before you begin:

- (Optional) Determine if a user account is locked by viewing their account status, as described in [View User Accounts](#).

To unlock a locked user account via the CLI:

1. In the command line interface (CLI) in Log Correlation Engine, run the following command:

```
/opt/lce/tools/user-utils --unlock--WebUI-acct <username>
```

Log Correlation Engine unlocks the user account.



Lock a User Account

Required User Role: Administrator

Users with locked accounts cannot login until an administrator unlocks their account. User accounts may be automatically locked if they do not follow the password reuse or login session policies an administrator configured. For more information about site policies, see [Site Policies](#).

For more information about user accounts, see [Users](#).

To lock a user account via the CLI:

1. Log in to Log Correlation Engine via the command line interface (CLI).
2. In the CLI in Log Correlation Engine, run the following command:

```
user-utils --lock--WebUI-acct <username>
```

Log Correlation Engine locks the user account.



Certificate-Authenticated Web UI Logins

You can configure the Log Correlation Engine server to allow certificate-authenticated connections for users logging in to the Log Correlation Engine web UI. When enabled, Log Correlation Engine requires certificate authentication for all users.

When you configure certificate-authenticated web UI logins:

- Users cannot log in to Log Correlation Engine using a username and password.
- Users cannot change their passwords.
- Log Correlation Engine continues to enforce the following site policy configuration attributes:
 - `web_UI__password__enforce_complexity`
 - `web_UI__password__minimum_length`
- Log Correlation Engine ignores the following site policy configuration attributes:
 - `web_UI__password__fewest_changes_ere_reuse`
 - `web_UI__password__minimum_edit_distance`
 - `web_UI__password__max_lifetime__days`
 - `web_UI__password__minimum_lifetime__hours`

For more information about site policy configuration attributes, see [Site Policies](#).

To fully configure certificate-authenticated web UI logins:

1. Configure the Log Correlation Engine server for certificate-authenticated logins, as described in [Configure Certificate-Authenticated Web UI Logins](#).
2. Configure certificate authentication for individual user accounts, as described in [Enable Certificate-Authenticated Web UI Logins for a User](#).



Configure Certificate-Authenticated Web UI Logins

Required User Role: Administrator

You can configure the Log Correlation Engine server to allow certificate-authenticated connections for users logging in to the Log Correlation Engine web UI. When enabled, Log Correlation Engine requires certificate authentication for all users.

To configure certificate-authenticated logins for the Log Correlation Engine web UI, you will need a certificate file representing one or more certificate authority (CA) entities you trust to sign certificates for your users. Typically, this is a `.pem` file.

For more information, see [Certificate-Authenticated Web UI Logins](#).

To configure certificate-authenticated web UI logins:

1. Log in to Log Correlation Engine via the command line interface (CLI).
2. In the CLI in Log Correlation Engine, run the following command:

```
/opt/lce/tools/cfg-utils --set-sv web_UI__login__client_CA_cert_path  
<the CA certificate>
```

Log Correlation Engine saves your configuration.

What to do next:

- Configure certificate authentication for individual user accounts, as described in [Enable Certificate-Authenticated Web UI Logins for a User](#).



Enable Certificate-Authenticated Web UI Logins for a User

Required User Role: Administrator

After you configure the Log Correlation Engine server for certificate-authenticated web UI logins, configure certificate authentication for each Log Correlation Engine user account. For more information, see [Certificate-Authenticated Web UI Logins](#).

Before you begin:

- Configure the Log Correlation Engine server to allow certificate-authenticated logins, as described in [Configure Certificate-Authenticated Web UI Logins](#).

To configure certificate authentication for a user account:

1. Log in to Log Correlation Engine via the command line interface (CLI).
2. In the CLI in Log Correlation Engine, run the following command:

```
/opt/lce/tools/cfg-utils --set-sv web_UI__login__client_CA_cert_path  
<the CA certificate>
```

Log Correlation Engine saves your configuration.



Disable Certificate-Authenticated WebUI Logins

Required User Role: Administrator

For more information, see [Certificate-Authenticated Web UI Logins](#).

To disable certificate-authenticated web UI logins:

1. Log in to Log Correlation Engine via the command line interface (CLI).
2. In the CLI in Log Correlation Engine, run the following command:

```
/opt/lce/tools/cfg-utils --set-sv web_UI__login__client_CA_cert_path ''
```

Log Correlation Engine saves your configuration.



Manage Clients in Tenable Log Correlation Engine

To access the **Clients** page:

- In the top navigation bar, click **Clients**.
- The **Clients** page displays a table of authorized clients and clients requesting permission to communicate with the Tenable Log Correlation Engine server.

This table is referred to throughout this documentation as the *client table*.

Caution: The Tenable Log Correlation Engine Client Manager Interactive Mode is deprecated. Clients should be managed using the **Clients** page.

The screenshot shows the LCE Clients page. At the top is a navigation bar with links for Health and Status, Configuration, Clients, Policies, and Users. The 'Clients' link is active. Below the navigation bar is a header for the 'Clients' section. Underneath is a table with columns: IP, Name, Type, OS, Policy, Version, and Last Heartbeat. A single client is listed with IP 172.26.20.67, Name unknown, Type LCE Splunk, OS RHEL 6, Policy default_rhel_icesplunk.lcp, Version 4.6.0.0, and Last Heartbeat 5 hours ago. The table has a 'Select all' checkbox, an 'Actions' dropdown, and a 'Search' input. There are also links for 'Advanced filters', 'Show 10 entries', and 'Show / hide columns'. At the bottom, it says 'Showing 1 to 1 of 1 entries' and has 'Previous', '1', and 'Next' buttons.

Additionally, the controls above the client table [allow you to search the entries in the client table, apply filters, and show or hide table columns](#).

Client operations in Tenable Log Correlation Engine are performed using the client table that is displayed on this page. Certain operations can be performed on one or more clients simultaneously by selecting the check boxes in the rows corresponding to the clients with which you want to interact.

The following table lists the columns that appear on the **Clients** page, and provides a brief description of each. Only certain columns are visible by default.

Column	Description
IP	The IP address of the Tenable Log Correlation Engine client host. If you have more than one client installed on a host, the same IP address will appear multiple times.
Name	The value in the name column will be one of the following, ordered by priority:



Column	Description
	<ul style="list-style-type: none">• The name you have assigned.• The hostname of the Tenable Log Correlation Engine client host, if resolved by the Tenable Log Correlation Engine server.• Unknown, only if a name is not assigned, and the Tenable Log Correlation Engine server cannot resolve the hostname.
Type	The type of Tenable Log Correlation Engine client. For example, LCE Splunk or LCE Client .
OS	<p>The operating system supported by the installed Tenable Log Correlation Engine client package.</p> <div>Note: While it may correspond, this value does not reflect the operating system installed on the host.</div>
Policy	The file name of the policy currently assigned to the Tenable Log Correlation Engine client.
Version	The version of the installed Tenable Log Correlation Engine client package.
Last Heartbeat	<p>The last time the Tenable Log Correlation Engine server received a heartbeat from an authorized Tenable Log Correlation Engine client.</p> <div>Tip: If you hover your cursor over this value, the exact timestamp appears.</div> <p>Unauthorized clients do not send heartbeats. This can be used to identify Tenable Log Correlation Engine clients that are not reporting to the Tenable Log Correlation Engine server correctly.</p>
Server	The IP address or hostname of the Tenable Log Correlation Engine server to which that Tenable Log Correlation Engine client is assigned. If the Tenable Log Correlation Engine client is installed on the same host as the Tenable Log Correlation Engine server, the IP addresses will be the same. By default, this column is not visible.
Authorized	Whether that Tenable Log Correlation Engine client is authorized to



Column	Description
	<p>communicate with the Tenable Log Correlation Engine server. By default, this column is not visible.</p> <div>Tip: This can be used to identify Tenable Log Correlation Engine clients that are not be reporting to the Tenable Log Correlation Engine server correctly.</div>
Alive	Whether a heartbeat or log was last received within the 5 minute reporting period from that client. By default, this column is not visible.
Logs today	The number of events received from that client today, including heartbeats. By default, this column is not visible.
UUID	The UUID of the client, if the client version supports UUIDs. The UUID is used to identify unique instances of Tenable Log Correlation Engine clients. By default, this column is not visible.



Clients Page Tasks

On the [Clients](#) page, you can do the following:

- [Authorize an Tenable Log Correlation Engine Client](#)
- [Revoke a Tenable Log Correlation Engine Client Authorization](#)
- [Delete a Tenable Log Correlation Engine Client](#)
- [Rename a Tenable Log Correlation Engine Client](#)
- [Assign a Policy to an Tenable Log Correlation Engine Client](#)
- [Assign an Tenable Log Correlation Engine Client to a Server](#)



Authorize an Tenable Log Correlation Engine Client

In order for an Tenable Log Correlation Engine client to communicate with a Tenable Log Correlation Engine server, it must first be authorized. Tenable Log Correlation Engine clients that have requested authorization appear in the client table.

Note: Client authorization is completed in the web-based Tenable Log Correlation Engine Interface on the Clients page.

To authorize a client to communicate with an Tenable Log Correlation Engine server:

1. Log in to Log Correlation Engine via the user interface.
2. In the top navigation bar, click **Clients**.

The **Clients** page appears, displaying the client table.

3. In the client table, in the rows corresponding to the Tenable Log Correlation Engine clients that you want to authorize, select the check boxes.

Tip: You can use filters or sort by the **Authorized** column to quickly find Tenable Log Correlation Engine clients that need to be authorized.

4. Above the client table, in the upper-left corner, click the **Actions** button, and then click **Authorize**.

The **Authorize** dialog box appears.

5. Review the list of Tenable Log Correlation Engine clients that will be authorized, and then click the **Authorize** button.

The Tenable Log Correlation Engine clients are authorized and will immediately send a heartbeat.



Additional Clients Page Tasks

This section details common tasks that are performed using the **Clients** page.

This section includes:

- [View Details About an Tenable Log Correlation Engine Client](#)
- [Select Multiple Client Table Entries](#)
- [Search the Client Table](#)
- [Add a Client Table Filter](#)
- [Clear Client Table Filters](#)
- [Limit the Client Table Entries Shown](#)
- [Show and Hide Client Table Columns](#)

View Details About an Tenable Log Correlation Engine Client

1. In the client table, click the row that corresponds to the Tenable Log Correlation Engine client for which you want to view details.

The **Detailed view** window appears, displaying a list of details about that Tenable Log Correlation Engine client. You can modify values in the **Name**, **Policy**, and **LCE server** boxes.

2. If you make changes to the Tenable Log Correlation Engine client details, click the **Update** button.

Log Correlation Engine saves your configuration..

Select Multiple Client Table Entries

There are two methods to select multiple entries in the client table:

- Above the client table, in the upper-left corner of the page, click the **Select all** button.
- In the rows corresponding to the Tenable Log Correlation Engine clients you want to select, click the check boxes.

Search the Client Table



- In the **Search** box, type a plain text search term. The **Search** box does not accept Boolean operators.

As you type, the client table will be filtered by your search term. The client table will search the text in all columns, regardless of whether they are shown or hidden.

Tip: If you are using the desktop version of Safari, you may need to disable the Correct Spelling Automatically function to prevent the browser from rewriting search terms.

Add a Client Table Filter

1. Above the client table, in the upper-left corner, click the **Actions** button, and then click **Add filter**.

The **Add new filter** dialog box appears.

2. In the **Filter on** box, select the column that contains the values you want to filter.

Depending on the column you select, the **Filter** box will appear as a text box or a list. For example, if you select **Authorized**, the **Filter** box is a list with the values Yes and No. If you select **Name**, you can type directly into the **Filter** box.

3. In the **Filter** box, type or select a value.
4. Click the **Add** button.

A new filter appears above the client table, and the client table is filtered based on the value.

Deselect all

Actions ▾

Client type: LCE Splunk ✕

Basic filter

Show 10 entries

Show / hide columns

IP	Name	Type	OS	Policy	Version	Last Heartbeat	
<input checked="" type="checkbox"/>	172.26.20.67	unknown	LCE Splunk	RHEL 6	default_rhel_lcesplunk.l...	4.6.0.0	20 hours ago

Showing 1 to 1 of 1 entries

Previous1Next

Clear Client Table Filters

There are two methods you can use to clear filters:

- Above the client table, in the box that represents the filter you want to clear, click the **x**. Repeat this process for each filter you want to clear.

Example:



Name: Splunk ✕

- Above the client table, in the upper-right corner, click the **Basic filter** link. All filters that you have applied to the client table are cleared.

Limit the Client Table Entries Shown

- Above the client table, in the upper-right corner, in the **Show** box, select the number of entries you want to show per client table page. By default, the **Show** box is set to *10*.

Show and Hide Client Table Columns

1. Above the client table, in the upper-right corner, click the **Show / hide columns** button.

A list of columns appears.

By default, the **Name**, **Type**, **OS**, **Policy**, **Version**, and **Last Heartbeat** columns are visible.

2. In the list of columns, select or clear the check boxes corresponding to the columns that you want to show or hide, respectively.

As you select and clear check boxes, the corresponding columns are either shown or hidden on the client table.



Rename a Tenable Log Correlation Engine Client

Naming a Tenable Log Correlation Engine client makes it easier to locate in the client table in the future. Initially, an Tenable Log Correlation Engine client is given one of the following names, ordered by priority:

- The hostname of the Tenable Log Correlation Engine client host, if resolved by the Tenable Log Correlation Engine server.
- *Unknown*, if a name is not assigned and the Tenable Log Correlation Engine server cannot resolve the hostname.

To rename an Tenable Log Correlation Engine Client:

1. Log in to Log Correlation Engine via the user interface.
2. In the top navigation bar, click **Clients**.

The **Clients** page appears, displaying the client table.

3. In the client table, in the row corresponding to the Tenable Log Correlation Engine client that you want to rename, select the check box.

Note: You can rename multiple Tenable Log Correlation Engine clients by selecting the corresponding check boxes. The selected clients will be assigned the same name.

4. Above the client table, in the upper-left corner, click the **Actions** button, and then click **Rename**.

The **Rename client(s)** dialog box appears.

5. In the **Name** box, type a name for the Tenable Log Correlation Engine client.
6. Review the Tenable Log Correlation Engine client that will be renamed, and then click the **Rename client(s)** button.

The Tenable Log Correlation Engine client is renamed. The new name appears in the **Name** column of the client table.



Assign a Policy to an Tenable Log Correlation Engine Client

In addition to using Tenable Security Center and the **Policies** page, you can assign policies to Tenable Log Correlation Engine clients via the **Clients** page.

To assign a policy to a client:

1. Log in to Log Correlation Engine via the user interface.
2. In the top navigation bar, click **Clients**.

The **Clients** page appears, displaying the client table.

3. In the client table, in the row corresponding to the Tenable Log Correlation Engine client that you want to assign a policy, select the check box.

Note: You can assign a policy to multiple Tenable Log Correlation Engine clients by selecting the corresponding check boxes. The selected Tenable Log Correlation Engine clients must be the same client type, and support the same operating system. The selected clients will be assigned the same policy.

4. Above the client table, in the upper-left corner, click the **Actions** button, and then click **Change Policy**.

The **Change policy** dialog box appears.

5. In the **Assign the following policy** list, select the policy that you want to assign to the Tenable Log Correlation Engine client.
6. Review the Tenable Log Correlation Engine client that will have a new policy, and then click the **Change policy** button.

The specified policy is assigned to the LCE client.



Assign an Tenable Log Correlation Engine Client to a Server

To assign a client to a server:

1. Log in to Log Correlation Engine via the user interface.
2. In the top navigation bar, click **Clients**.

The **Clients** page appears, displaying the client table.

3. In the client table, in the rows corresponding to the Tenable Log Correlation Engine clients that you want to assign to a different Tenable Log Correlation Engine server, select the check boxes.
4. Above the client table, in the upper-left corner, click the **Actions** button, and then click **Assign to..**

The **Assign server** dialog box appears.

By default, below the list of Tenable Log Correlation Engine clients, the first box is set to *IP address*.

5. If you want to use a hostname, in the first box, select **Hostname**, and then type a hostname. Otherwise, type an IP address.
6. In the **Port** box, type the port number for the LCE server. Unless the Tenable Log Correlation Engine server has been configured to use a different port, the default Tenable Log Correlation Engine Client port is *31300*.
7. Review the list of Tenable Log Correlation Engine clients that will be assigned to a new Tenable Log Correlation Engine server, and then click the **Assign server** button.

The Tenable Log Correlation Engine clients are assigned to the specified Tenable Log Correlation Engine server.



Revoke a Tenable Log Correlation Engine Client Authorization

To revoke a client authorization:

1. Log in to Log Correlation Engine via the user interface.
2. In the top navigation bar, click **Clients**.

The **Clients** page appears, displaying the client table.

3. In the client table, in the rows corresponding to the Tenable Log Correlation Engine clients that have authorizations you want to revoke, select the check boxes.
4. Above the client table, in the upper-left corner, click the **Actions** button, and then click **Revoke**.

The **Revoke** dialog box appears.

5. Review the list of Tenable Log Correlation Engine clients that will have authorizations revoked, and then click the **Revoke** button.

The authorizations for the Tenable Log Correlation Engine clients are revoked. The Tenable Log Correlation Engine clients will no longer be able to communicate with the Tenable Log Correlation Engine server, except to request authorization.



Delete a Tenable Log Correlation Engine Client

When you delete a Tenable Log Correlation Engine client on the **Clients** page, the Tenable Log Correlation Engine client is not uninstalled from its host, only removed from the client table. If the Tenable Log Correlation Engine client was authorized, the authorization will be revoked when it is deleted.

To delete a client on the **Clients** page:

1. Log in to Log Correlation Engine via the user interface.
2. In the top navigation bar, click **Clients**.

The **Clients** page appears, displaying the client table.

3. In the client table, in the rows corresponding to the Tenable Log Correlation Engine clients that you want to delete, select the check boxes.
4. Above the client table, in the upper-left corner, click the **Actions** button, and then click **Delete**.

The **Delete** dialog box appears.

5. Review the list of Tenable Log Correlation Engine clients that will be deleted, and then click the **Delete** button.

The Tenable Log Correlation Engine clients are removed from the client table. If any of those clients were authorized, that authorization is revoked.



Client Policies

To access the **Policies** page, in the top navigation bar, click **Policies**. The **Policies** page appears, displaying a table of policies, including the pre-packaged default and TNS policies. This table is referred to throughout this documentation as the *policy table*.

The **Policies** page is used to perform the following tasks:

- [Create client policies](#)
- [Edit client policies](#)
- [Clone client policies](#)
- [Delete client policies](#)
- [Download client policies](#)
- [Upload client policies](#)

Creating, editing, and cloning policies is performed using the [Client Policy Builder](#).

Additionally, using the controls above the policy table, [you can search the entries in the policy table, and show or hide table columns](#).

The following table lists the columns that appear on the **Policies** page, and provides a brief description of each. By default, all columns are visible.

Column	Description
Policy name	The file name of the policy. The name of a prepackaged policy is prefixed by <i>default</i> or <i>TNS</i> . All policy files for Tenable Log Correlation Engine have the <i>.lcp</i> extension.
OS	The operating system supported by the policy.
Client Type	The type of Tenable Log Correlation Engine client that the policy is for. For example, <i>LCE Splunk</i> or <i>LCE Client</i> .
Clients using	The number of clients to which the policy is assigned.
Created by	The user who created the policy. In the case of the prepackaged policies, the



Column	Description
	value is <i>Ice</i> .
Last modified by	The user who last modified the policy.
Created on	The date on which the policy was created, or, if within 24 hours, the time since the policy was created. For example, <i>16 hours ago</i> .
Actions	Contains the Edit , Clone , Delete , and Download buttons.

List All Client Policies

You can list all client policies with `/opt/lce/tools/list-policies`. For more information about the list-policies tool, see [list-policies](#).

Example output:



basename	agent	tCreated	fileMD5
TNS-TenableProducts-PVS_rhel_lceclient.lcp	tailLnx	2021, Jan04, 15:43:14	9a926de0b5d5b81285ddf35b98138f28
default_rhel_opsec.lcp	OPSEC	2021, Jan04, 15:43:14	a6b732ddb526341f3d5d9f48cd218a8
TNS-NEvents-FileSysMon_windows_tenableclient.lcp	tailWin	2021, Jan04, 15:43:14	a8da8f78ea449e609958c03c9d1c4a90
default_rhel_sdee.lcp	SDEE	2021, Jan04, 15:43:14	84d922f0a1aa8c5cb326cbd30ee79aae
TNS-MalwareDetectionOnly_osx_lceclient.lcp	tailLnx	2021, Jan04, 15:43:14	ce1d7345e9b7e2e9a18eadebf3c0f5a42
default_appliance_networkmonitor.lcp	NetwMon	2021, Jan04, 15:43:14	ed2c4fbe798e60ea88d290a523e99216
default_appliance_netflowclient.lcp	NetFlow	2021, Jan04, 15:43:14	23119fd6ac77d22fb30eb6c94713ce87
TNS-ProcessExecutionOnly_rhel_lceclient.lcp	tailLnx	2021, Jan04, 15:43:14	aa22d33c92e74a7128c5b42874f80de6
TNS-TenableProducts-Nessus_windows_tenableclient.lcp	tailWin	2021, Jan04, 15:43:14	8b02124aae8a940d4568b35a66f52a93
default_aix_lceclient.lcp	tailLnx	2021, Jan04, 15:43:14	862772fbfb862e7389c48f94c5f3501
TNS-MSSQLServer_windows_tenableclient.lcp	tailWin	2021, Jan04, 15:43:14	2d5930f84d17960c724ecada204027ee
TNS-MalwareDetectionOnly_rhel_lceclient.lcp	tailLnx	2021, Jan04, 15:43:14	c710543b52611148afccb7aa46fac8e0
default_appliance_lceclient.lcp	tailLnx	2021, Jan04, 15:43:14	0a3bc0fba520b6061de6fe253046adb
default_windows_reserved.lcp	<test>	2021, Jan04, 15:43:14	624fbc3965a017cf0a89cb6727b06d5f
default_suse_lceclient.lcp	tailLnx	2021, Jan04, 15:43:14	936b7b6af59086c0e9b05eb24ca79fb2
TNS-NEvents_windows_tenableclient.lcp	tailWin	2021, Jan04, 15:43:14	f7e1bde656c0dd853ca7788f67012aed
default_rhel_rdep.lcp	RDEP	2021, Jan04, 15:43:14	2158ef30a797b179daa11c41e2b126e
TNS-TenableProducts-LCE_rhel_lceclient.lcp	tailLnx	2021, Jan04, 15:43:14	c8c683e55ba0199e2dae20dc413e84a7
TNS-MalwareDetectionOnly_windows_tenableclient.lcp	tailWin	2021, Jan04, 15:43:14	f52e692134d855af0f5877dde6958b9f
default_osx_lceclient.lcp	tailLnx	2021, Jan04, 15:43:14	a849c747a13ca9a1c47c0937b627b03f
default_rhel_lceclient.lcp	tailLnx	2021, Jan04, 15:43:14	340dfad1141fa47bf7e89ab13a6ad043
default_windows_tenableclient.lcp	tailWin	2021, Jan04, 15:43:14	91d23748e962414eedf523d58e738829
default_rhel_netflowclient.lcp	NetFlow	2021, Jan04, 15:43:14	acf7b17e9d354988295aa02580e5c883
TNS-MSEXchangeServer_windows_tenableclient.lcp	tailWin	2021, Jan04, 15:43:14	ee41a2cc0be6a4ac72193c66111eea02
default_rhel_web.lcp	Web	2021, Jan04, 15:43:14	1c14fb1f506fb1ddbe24acb14372a167
default_debian_lceclient.lcp	tailLnx	2021, Jan04, 15:43:14	daf0e38c28cb413b68ee55d74e5a39b6
default_dragon_lceclient.lcp	tailLnx	2021, Jan04, 15:43:14	efae379b3afac0905a855f12ff037a55
default_ubuntu_lceclient.lcp	tailLnx	2021, Jan04, 15:43:14	6debc7823c7577ca18e37aaa34003ad1
TNS-TenableProducts-SC_rhel_lceclient.lcp	tailLnx	2021, Jan04, 15:43:14	489da59f56b7f1ea120b3d2b4217e389
TNS-ProcessExecutionOnly_windows_tenableclient.lcp	tailWin	2021, Jan04, 15:43:14	2642146c6ee4792f84a8befbe8722750
default_freebsd_lceclient.lcp	tailLnx	2021, Jan04, 15:43:14	cb75f0586972e5220e401773abb19dfa
TNS-TenableProducts-Nessus_rhel_lceclient.lcp	tailLnx	2021, Jan04, 15:43:14	2bfff42edf1068c2286a0ce11a66df963
TNS-TenableProducts_rhel_lceclient.lcp	tailLnx	2021, Jan04, 15:43:14	6b6f774009371b9ac651949d0dd71893
default_hpux_lceclient.lcp	tailLnx	2021, Jan04, 15:43:14	0d867fdd406c55d1de568f8124c8b001
default_rhel_networkmonitor.lcp	NetwMon	2021, Jan04, 15:43:14	af6aa96cf8cdb769bb0f2c2a07ce5d95
default_rhel_wmimonitor.lcp	WMI	2021, Jan04, 15:43:14	618ac4dbbeadf2c6f06d06a1d2471486
TNS-WinDesktop_windows_tenableclient.lcp	tailWin	2021, Jan04, 15:43:14	8c71529bffb2a1471b10d7eaa6295208
default_solaris_lceclient.lcp	tailLnx	2021, Jan04, 15:43:14	0dbfb2a1af3863eca17d3af9fd2825e4
default_rhel_lcesplunk.lcp	Splunk	2021, Jan04, 15:43:14	eea31b45d361ad57d0a6d8f581fca6e2
TNS-ProcessExecutionOnly_osx_lceclient.lcp	tailLnx	2021, Jan04, 15:43:14	0eb804f2acc1431d122de5c119a658e2
default_fedora_lceclient.lcp	tailLnx	2021, Jan04, 15:43:14	07b551b38753ca1a2bbcb78c79cbdfc
zsuperchatty_windows_tenableclient.lcp	tailWin	2021, Jan15, 17:30:13	ecd38181bcecd9c5f3a14d0eea90c606
zchatty_rhel_networkmonitor.lcp	NetwMon	2021, Jan15, 17:30:13	49bd4c558c14b054d3f6a7534c56687d
bunniesZZ_osx_lceclient.lcp	tailLnx	2021, Jan22, 15:53:38	f8d1f5fc8d930a05299eaab6ecf85ef6
bunniesYY_windows_tenableclient.lcp	tailWin	2021, Jan22, 15:54:45	c37527ee34f7e282e94348cd01da6c47
bunniesZZ_solaris_lceclient.lcp	tailLnx	2021, Jan22, 16:00:22	7832ad66059be6130a4977970f9a8a8f



Client Policy Builder

The Client Policy Builder is a tool for creating and editing policies directly in the Tenable Log Correlation Engine interface. The Builder can be used to create a policy for any supported combination of Tenable Log Correlation Engine client and operating system, and will not allow invalid combinations, preventing you from inadvertently creating an invalid policy. Additionally, if upgrading from a previous version of Tenable Log Correlation Engine, the Builder can be used to modify any existing policies and will alert you if an existing policy that you modify is invalid.

The screenshot shows the Client Policy Builder interface. The title bar at the top includes the LCE logo, navigation icons for Health and Status, Configuration, Clients, Policies, and Users, and a user dropdown menu showing 'admin'. Below the title bar, the current policy is 'default_rhel_networkmonitor.lcp - Network Monitor, RHEL'. There are three buttons: 'Save', 'Save as..', and 'Quit'. The interface is divided into two panes: 'Basic' and 'Advanced'.

Basic Pane:

- Interface:** eth0
- Included networks:** Filter
- Excluded networks:** Filter
- Monitor syslog port:** udp/514, tcp/1468
- Syslog only:** ☐
- Filter expression:** No value defined.
- Log directory:** ☒
- Client heartbeat frequency:** 300
- Client statistics frequency:** 60
- Compress events:** ☒

Advanced Pane:

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<!-- Created with LCE web policy editor by user admin -->
<options xmlns:xi="http://www.w3.org/2003/XInclude">
  <interface>eth0</interface>
  <include-networks>
    <filter>10.0.0.0/8</filter>
    <filter>192.168.0.0/16</filter>
    <filter>172.16.0.0/12</filter>
    <filter>127.0.0.1</filter>
  </include-networks>
  <exclude-networks>
    <filter>203.0.113.0/24</filter>
  </exclude-networks>
  <monitor-syslog-port>udp/514</monitor-syslog-port>
  <monitor-syslog-port>tcp/1468</monitor-syslog-port>
  <syslog-only>no</syslog-only>
  <log-directory>./</log-directory>
  <heartbeat-frequency>300</heartbeat-frequency>
  <statistics-frequency>60</statistics-frequency>
  <compress-events>1</compress-events>
</options>
```

The Builder is divided into the title bar and the **Basic** and **Advanced** panes.

In the **Basic** pane:

You can add or remove configuration items and specify valid values for those items. All values that you enter for configuration items are validated. If an invalid value is entered, the Builder warns you and prevents the invalid policy from being saved. As you modify the configuration items in the **Basic** pane, the XML source code in the **Advanced** pane will be updated to reflect the new values. In the **Basic** pane, if a check box is empty, the value for that configuration item will be set to *false* in the **Advanced** pane.

In the **Advanced** pane:



You can modify the XML directly. As with the values in the **Basic** pane, all changes made to the XML are validated, including but not limited to values for the configuration items, element tags, and the file header. You are also alerted if you attempt to add configuration items that do not correspond to the policy type. When changes are made to values in the XML, the **Basic** pane is updated to reflect the new values.

Note: It is recommended that only advanced users utilize the **Advanced** pane.



Create a Client Policy with the Client Policy Builder

To create a client policy with the client policy builder:

1. Log in to Log Correlation Engine via the user interface.
2. In the top navigation bar, click **Policies**.

The **Policies** page appears, displaying the policy table.

Policy name	OS	Client type	Clients using	Author	Modified by	Created	Modified on
default_adx_lceclient.lcp	ADX	LCE Client	0	lce	-	5 days ago	-
default_appliance_lceclient.lcp	Tenable Appliance	LCE Client	0	lce	-	5 days ago	-
default_appliance_netflowclient.lcp	Tenable Appliance	Netflow Client	0	lce	-	5 days ago	-
default_appliance_networkmonitor.lcp	Tenable Appliance	Network Monitor	0	lce	-	5 days ago	-
default_debian_lceclient.lcp	Debian	LCE Client	0	lce	-	5 days ago	-
default_dragon_lceclient.lcp	Dragon	LCE Client	0	lce	-	5 days ago	-
default_fedora_lceclient.lcp	Fedora	LCE Client	0	lce	-	5 days ago	-
default_freebsd_lceclient.lcp	FreeBSD	LCE Client	0	lce	-	5 days ago	-
default_hpux_lceclient.lcp	HP-UX	LCE Client	0	lce	-	5 days ago	-
default_osx_lceclient.lcp	OS X	LCE Client	0	lce	-	5 days ago	-

3. In the upper-left corner of the policy table, click the **Add policy** button.

The **Client Policy Builder** window appears, displaying the **Create** section.

4. In the **OS** list, select the operating system of the host for which you want to create a policy.

The **Client** list is filtered automatically to display only Tenable Log Correlation Engine clients that are supported on the select operating system. For example, if you select *Windows*, the **Client** list will be limited to just *Tenable Client*, the only supported Tenable Log Correlation Engine client for Windows.

5. In the **Client** list, select the client for which you want to create a policy, and then click the **Start Editing** button.

The Client Policy Builder appears. At the top of the Builder, the title bar displays the name of the default policy corresponding to the operating system and Tenable Log Correlation Engine client that you selected. A complete list of configuration items that are valid for the type of



policy appear in the **Basic** pane. XML source code with corresponding values appears in the **Advanced** pane.

default_rhel_networkmonitor.lcp - Network Monitor, RHEL

Save

+ Save as...

Quit

Basic

Advanced

Interface

eth0

Included networks

Filter

Excluded networks

Filter

Monitor syslog port

udp/514

tcp/1468

Syslog only: ☐

Filter expression: No value defined.

Log directory: ☒

Client heartbeat frequency: 300

Client statistics frequency: 60

Compress events: ☒

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<!-- Created with LCE web policy editor by user admin -->
<options xmlns:xi="http://www.w3.org/2003/XInclude">
  <interface>eth0</interface>
  <include-networks>
    <filter>10.0.0.0/8</filter>
    <filter>192.168.0.0/16</filter>
    <filter>172.16.0.0/12</filter>
    <filter>127.0.0.1</filter>
  </include-networks>
  <exclude-networks>
    <filter>203.0.113.0/24</filter>
  </exclude-networks>
  <monitor-syslog-port>udp/514</monitor-syslog-port>
  <monitor-syslog-port>tcp/1468</monitor-syslog-port>
  <syslog-only>no</syslog-only>
  <log-directory>./</log-directory>
  <heartbeat-frequency>300</heartbeat-frequency>
  <statistics-frequency>60</statistics-frequency>
  <compress-events>1</compress-events>
</options>
```

Note: The list of configuration items in the **Basic** pane includes items that do not yet have a configured value. If the configuration item normally accepts a value, *No value defined* will be displayed. In the case of a group, that group will not contain any items.

6. Using the **Basic** or **Advanced** panes, modify values for each configuration item.

Tip: In the **Basic** pane, to modify a configuration item that uses a list of values (e. g., **Included networks**), click **+** to add items and **-** to remove items from the list. Additionally, to expand and collapse the lists, click **▢** and **▤**, respectively. If configuration items are visible in the **Advanced** pane but not in the **Basic** pane, it is likely that the parent configuration item is currently collapsed.

As you configure the policy, the Builder will validate the configuration items, and alert you if any invalid configuration is found.

7. Click the **Save as** button.

The **Save file as** dialog box appears.

8. In the **Filename** box, type a name for the policy. A valid file name cannot include the phrase *default* or *TNS* as a prefix, and cannot include spaces or underscores. Do not include a file extension. The operating system, client, and file extension will be appended to the name when



the policy is saved.

For example, if you are saving a policy for the Tenable Log Correlation Engine Tenable Network Monitor that supports Red Hat Enterprise Linux, and you type *corpnet* as the name, the policy will be saved with the following complete name: *corpnet_rhel_networkmonitor.lcp*.

Note: The policy name can be a maximum of 50 characters.

9. Click **OK**.

Log Correlation Engine saves your configuration.

A notification appears, confirming that the policy was saved successfully. The **Save** button is enabled. You can continue to modify the policy and save those changes.

10. At the top of the Builder, in the title bar, click the **Quit** button.

The **Policies** page appears, displaying a list of default and existing policies.



Edit a Client Policy with the Client Policy Builder

To edit a client policy with the client policy builder:

1. Log in to Log Correlation Engine via the user interface.
2. In the top navigation bar, click **Policies**.

The **Policies** page appears, displaying the policy table.

Policy name	OS	Client type	Clients using	Author	Modified by	Created	Modified on
default_adx_lceclient.lcp	ADX	LCE Client	0	lce	-	5 days ago	-
default_appliance_lceclient.lcp	Tenable Appliance	LCE Client	0	lce	-	5 days ago	-
default_appliance_netflowclient.lcp	Tenable Appliance	Netflow Client	0	lce	-	5 days ago	-
default_appliance_networkmonitor.lcp	Tenable Appliance	Network Monitor	0	lce	-	5 days ago	-
default_debian_lceclient.lcp	Debian	LCE Client	0	lce	-	5 days ago	-
default_dragon_lceclient.lcp	Dragon	LCE Client	0	lce	-	5 days ago	-
default_fedora_lceclient.lcp	Fedora	LCE Client	0	lce	-	5 days ago	-
default_freebsd_lceclient.lcp	FreeBSD	LCE Client	0	lce	-	5 days ago	-
default_hpux_lceclient.lcp	HP-UX	LCE Client	0	lce	-	5 days ago	-
default_osx_lceclient.lcp	OS X	LCE Client	0	lce	-	5 days ago	-

3. In the row corresponding to the policy you want to edit, in the **Actions** column, click the **Edit** button.

The Client Policy Builder appears. At the top of the Builder, the title bar displays the name of the policy that you selected. A complete list of configuration items that are valid for the type of policy appear in the **Basic** pane. XML source code with corresponding values appears in the **Advanced** pane.

Caution: If comments are present in an existing policy, those comments will be removed. Comments will not be saved with the policy.

4. Using the **Basic** or **Advanced** panes, modify values for each configuration item.

Tip: In the **Basic** pane, to modify a configuration item that uses a list of values (e. g., **Included networks**), click to add items and to remove items from the list. Additionally, to expand and collapse the lists, click and , respectively. If configuration items are visible in the



Advanced pane, but not in the **Basic** pane, it is likely that the parent configuration item is currently collapsed.

As you configure the policy, the Builder will validate the configuration items, and alert you if any invalid configuration is found.

5. If you want to keep the existing file name, click the **Save** button, and then proceed to step 7 of this procedure. Otherwise, click the **Save as** button.

The **Save file as** dialog box appears.

6. In the **Filename** box, type a name for the policy. Do not include a file extension. The operating system, client, and file extension will be appended to the name when the policy is saved.

For example, if you are saving a policy for the Tenable Log Correlation Engine Tenable Network Monitor that supports Red Hat Enterprise Linux, and you type *corpnet* as the name, the policy will be saved with the following complete name: *corpnet_rhel_networkmonitor.lcp*.

7. Click **OK**.

Log Correlation Engine saves your configuration.

A notification appears, confirming that the policy was saved successfully.

8. At the top of the Builder, in the title bar, click the **Quit** button.

The **Policies** page appears, displaying a list of default and existing policies. To confirm that the policy you modified was saved, in the upper-right corner of the list of policies, in the **Search** box, type the name of the policy you created, and then check the value in the **Last modified on** column.



Upload a Client Policy

It is recommended that you create and modify policies using the [Client Policy Builder](#), but if desired, you can still download a policy in order to modify it and then upload the modified policy back into the Tenable Log Correlation Engine server.

To upload a client policy or upload a modified client policy:

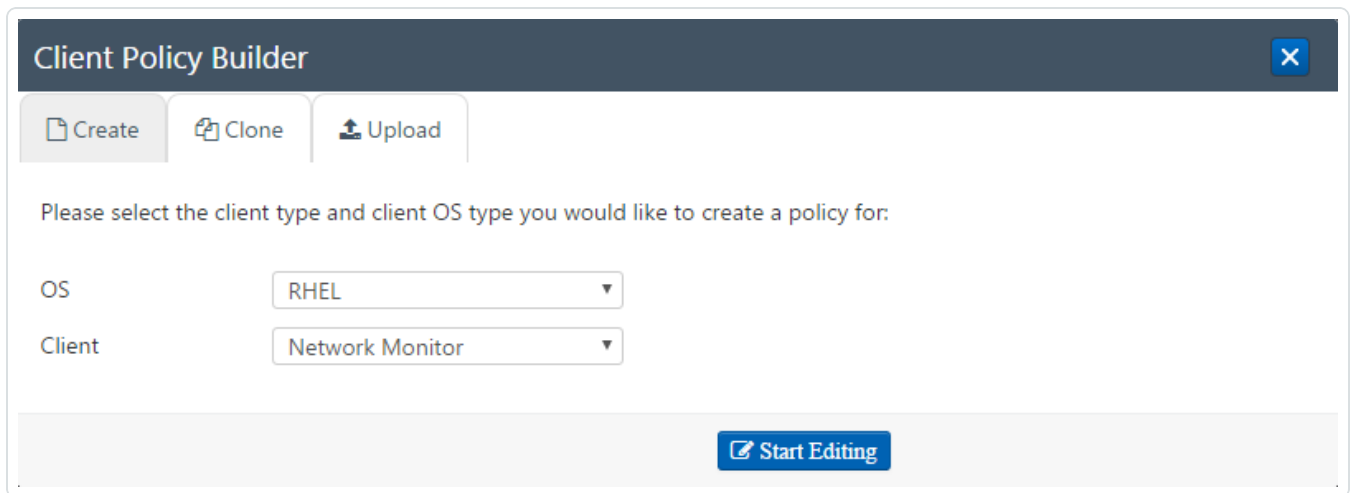
1. Log in to Log Correlation Engine via the user interface.
2. In the top navigation bar, click **Policies**.

The **Policies** page appears, displaying the policy table.

LCE log correlation engine							
Health and Status Configuration Clients Policies Users admin							
Policies							
Add policy Search: Show 10 entries Show / hide columns							
Policy name	OS	Client type	Clients using	Author	Modified by	Created	Modified on
default_aix_lceclient.lcp	AIX	LCE Client	0	Ice	-	a day ago	-
default_appliance_lceclient.lcp	Tenable Appliance	LCE Client	0	Ice	-	a day ago	-
default_appliance_netflowclient.lcp	Tenable Appliance	Netflow Client	0	Ice	-	a day ago	-
default_appliance_networkmonitor.lcp	Tenable Appliance	Network Monitor	0	Ice	-	a day ago	-
default_debian_lceclient.lcp	Debian	LCE Client	0	Ice	-	a day ago	-
default_dragon_lceclient.lcp	Dragon	LCE Client	0	Ice	-	a day ago	-
default_fedora_lceclient.lcp	Fedora	LCE Client	0	Ice	-	a day ago	-
default_freebsd_lceclient.lcp	FreeBSD	LCE Client	0	Ice	-	a day ago	-
default_hpux_lceclient.lcp	HP-UX	LCE Client	0	Ice	-	a day ago	-
default_osx_lceclient.lcp	OS X	LCE Client	0	Ice	-	a day ago	-
Showing 1 to 10 of 40 entries						Previous	1 2 3 4 Next

3. In the upper-left corner of the policy table, click the **Add policy** button.

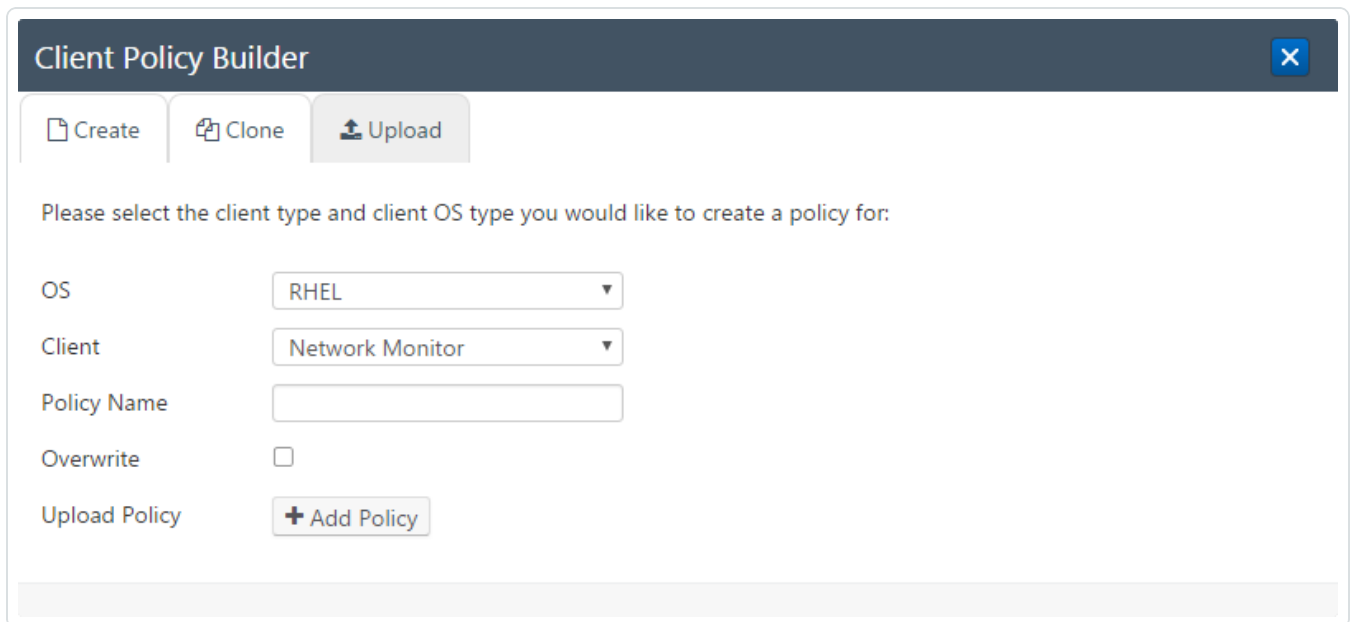
The **Client Policy Builder** window appears, displaying the **Create** section.



The image shows a 'Client Policy Builder' dialog box with a dark header bar containing a close button (X). Below the header, there are three tabs: 'Create', 'Clone', and 'Upload'. The 'Create' tab is currently selected. The main content area contains the text 'Please select the client type and client OS type you would like to create a policy for:'. Below this text are two dropdown menus: 'OS' with 'RHEL' selected, and 'Client' with 'Network Monitor' selected. At the bottom right of the dialog, there is a blue button labeled 'Start Editing'.

4. Click the **Upload** tab.

The **Upload** section appears.



The image shows the 'Client Policy Builder' dialog box with the 'Upload' tab selected. The 'OS' dropdown is set to 'RHEL' and the 'Client' dropdown is set to 'Network Monitor'. Below these, there is a text input field for 'Policy Name'. An 'Overwrite' checkbox is present and is currently unchecked. At the bottom, there is a button labeled '+ Add Policy' next to the 'Upload Policy' label.

5. In the **OS** list, select the operating system corresponding to the client policy you want to upload.
6. In the **Client** list, select the type of Tenable Log Correlation Engine client corresponding to the client policy you want to upload.

Note: The selected OS and Client *must* match the policy you want to upload, or the upload will fail and an error message will appear.



7. In the **Policy Name** box, type a name for the policy. A valid policy name cannot include the phrase *default* or *TNS* as a prefix, and cannot include spaces or underscores. Do not include a file extension. The operating system, client, and file extension will be appended to the name when the policy is saved.

For example, if you are uploading a policy for the Tenable Log Correlation Engine Tenable Network Monitor that supports Red Hat Enterprise Linux, and you type *corpnet* as the name, the policy will be uploaded with the following complete name: *corpnet_rhel_networkmonitor.lcp*.

8. If you want to overwrite an existing policy that has the same name, select the **Overwrite** check box.
9. Click the **Add Policy** button.

The policy is uploaded and appears in the policy table.



Download a Client Policy

It is recommended that you create and modify policies using the [Client Policy Builder](#), but if desired, you can still download a policy in order to modify it or transfer it to another Tenable Log Correlation Engine server.

To download a client policy:

1. Log in to Log Correlation Engine via the user interface.
2. In the top navigation bar, click **Policies**.

The **Policies** page appears, displaying the policy table.

3. In the policy table, in the row corresponding to the policy that you want to download, click the **Download** button.

The policy is downloaded. If desired, you can make changes, and then [upload the policy](#).



Clone a Client Policy with the Client Policy Builder

To clone a client policy with the client policy builder:

1. Log in to Log Correlation Engine via the user interface.
2. In the top navigation bar, click **Policies**.

The **Policies** page appears, displaying the policy table.

The screenshot shows the LCE (Log Correlation Engine) interface. The top navigation bar includes links for Health and Status, Configuration, Clients, Policies (selected), and Users. The user is logged in as 'admin'. The main section is titled 'Policies' and contains a table of client policies. The table has columns for Policy name, OS, Client type, Clients using, Author, Modified by, Created, and Modified on. There are 10 entries in the table, all with 'Ice' as the author and '5 days ago' as the creation/modification date. The table is paginated, showing 1 to 10 of 40 entries.

Policy name	OS	Client type	Clients using	Author	Modified by	Created	Modified on
default_atix_lceclient.lcp	ADX	LCE Client	0	Ice	-	5 days ago	-
default_appliance_lceclient.lcp	Tenable Appliance	LCE Client	0	Ice	-	5 days ago	-
default_appliance_netflowclient.lcp	Tenable Appliance	Netflow Client	0	Ice	-	5 days ago	-
default_appliance_networkmonitor.lcp	Tenable Appliance	Network Monitor	0	Ice	-	5 days ago	-
default_debian_lceclient.lcp	Debian	LCE Client	0	Ice	-	5 days ago	-
default_dragon_lceclient.lcp	Dragon	LCE Client	0	Ice	-	5 days ago	-
default_fedora_lceclient.lcp	Fedora	LCE Client	0	Ice	-	5 days ago	-
default_freebsd_lceclient.lcp	FreeBSD	LCE Client	0	Ice	-	5 days ago	-
default_hpux_lceclient.lcp	HP-UX	LCE Client	0	Ice	-	5 days ago	-
default_osx_lceclient.lcp	OS X	LCE Client	0	Ice	-	5 days ago	-

3. In the row corresponding to the policy you want to clone, in the **Actions** column, click the **Clone** button.

-or-

- a. In the upper-left corner of the policy table, click the **Add policy** button.

The **Client Policy Builder** window appears, displaying the **Create** section.



Client Policy Builder

Create

Clone

Upload

Please select the client type and client OS type you would like to create a policy for:

OS

RHEL

Client

Network Monitor

Start Editing

- b. Click the **Clone** tab.

The **Clone** section appears.

Client Policy Builder

Create

Clone

Upload

Select an existing policy to use as a starting point:

Policy







default_rhel_icesplunk.lcp

Start editing

- c. In the **Policy** list, select the policy that you want to clone, and then click the **Start Editing** button.

The Client Policy Builder appears. At the top of the Builder, the title bar displays the name of the policy that you selected. A complete list of configuration items that are valid for the type of policy appear in the **Basic** pane. XML source code with corresponding values appears in the **Advanced** pane.

4. Using the **Basic** or **Advanced** panes, modify values for each configuration item.

Tip: In the **Basic** pane, to modify a configuration item that uses a list of values (e. g., **Included networks**  ), click  to add items and  to remove items from the list. Additionally, to expand and collapse the lists, click  and , respectively. If configuration items are visible in the



Advanced pane, but not in the **Basic** pane, it is likely that the parent configuration item is currently collapsed.

As you configure the policy, the Builder will validate the configuration items and alert you if any invalid configuration is found.

5. Click the **Save as** button.

The **Save file as** dialog box appears.

6. In the **Filename** box, type a name for the policy. Do not include a file extension. The operating system, client, and file extension will be appended to the name when the policy is saved.

For example, if you are saving a policy for the Tenable Log Correlation Engine Tenable Network Monitor that supports Red Hat Enterprise Linux, and you type *corpnet* as the name, the policy will be saved with the following complete name: *corpnet_rhel_networkmonitor.lcp*.

7. Click **OK**.

Log Correlation Engine saves your configuration.

A notification appears, confirming that the policy was saved successfully. The **Save** button is enabled. You can continue to modify the policy and save those changes.

8. At the top of the Builder, in the title bar, click the **Quit** button.

The **Policies** page appears, displaying a list of default and existing policies.



Other Policies Page Tasks

This section details common tasks that are performed using the **Policies** page.

This section includes:

- [Search the Policy Table](#)
- [Limit the Policy Table Entries Shown](#)
- [Show and Hide Policy Table Columns](#)

Search the Policy Table

- Above the policy table, in the **Search** box, type a plain text search term. The **Search** box does not accept Boolean operators.

As you type, the policy table is filtered by your search term. The text in all columns of the policy table is searched, regardless of whether they are shown or hidden.

Tip: If you are using the desktop version of Safari, you may need to disable the Correct Spelling Automatically function to prevent the browser from rewriting search terms.

Limit the Policy Table Entries Shown

- Above the policy table, in the upper-right corner, in the **Show** box, select the number of entries you want to show per policy table page. By default, the **Show** box is set to 10.

Show and Hide Policy Table Columns

1. Above the policy table, in the upper-right corner, click the **Show / hide columns** button.

A list of columns appears.

By default, all columns are visible.

2. In the list of columns, select or clear the check boxes corresponding to the columns that you want to show or hide, respectively.

As you select and clear check boxes, the policy table is updated with the appropriate columns.



Delete a Client Policy

You cannot delete policies that are currently being used by clients, or pre-packaged policies (i. e., *default* and *TNS* policies). Policies are deleted permanently and cannot be recovered.

To delete a client policy:

1. Log in to Log Correlation Engine via the user interface.
2. In the top navigation bar, click **Policies**.

The **Policies** page appears, displaying the policy table.

3. In the policy table, in the row corresponding to the policy that you want to delete, click the **Delete** button.

The **Confirm deletion** dialog box appears.

4. Click **OK**.

The policy is deleted.



Automatically Authorize Tenable Log Correlation Engine Clients

In order for an Tenable Log Correlation Engine client to communicate with a Tenable Log Correlation Engine server, it must first be authorized. Client assignment rules can be used to automatically authorize clients.

To auto authorize a Tenable Log Correlation Engine to communicate with a Tenable Log Correlation Engine server:

1. Log in to Log Correlation Engine via the user interface.
2. In the top navigation bar, click **Configuration**.

The **System Configuration** page appears, displaying basic configuration settings.

3. In the left side navigation bar, click **Advanced**.

The **Advanced** configuration section appears, displaying options used to fine tune your Tenable Log Correlation Engine server configuration.

4. Scroll down to the **Clients** section, and check the **Auto Authorize** checkbox.
5. Enter a network range in the **Client Network** field using CIDR notation.
6. In the **LCE IP:port** field, enter the Tenable Log Correlation Engine server IP address and port that you want the clients to communicate with.
7. Click the **Add New Client Rule** button.
The policies text box appears.
8. In the text box, specify the filenames of the policies that you want applied to clients that fall in the range defined by the rule.

Note: Policies are matched by operating system. If there are multiple policies for a particular operating system, the first applicable policy that is specified for that operating system will be assigned. If none of the specified policies are applicable to a client in the network, the default policy for that operating system will be used.

9. Scroll to the bottom of the page and click the **Update** button.

Log Correlation Engine saves your configuration.

Tip: Install the Tenable Log Correlation Engine client on your target hosts if you haven't already.



Tenable Log Correlation Engine Clients

A key component of Tenable Log Correlation Engine, clients capture event data from a variety of sources and send that data to the Tenable Log Correlation Engine server for normalization. The Tenable Log Correlation Engine clients are installed on systems whose logs, network traffic, performance and other types of protocols and technologies are to be monitored by forwarding the data securely to the Tenable Log Correlation Engine server. Policies are assigned to the Tenable Log Correlation Engine clients, which govern the methods by which a client captures event data. For example, the Web Query Client is used to collect events from Salesforce, AWS CloudTrail, and Google Cloud Platform.

The following table lists the Tenable Log Correlation Engine clients that Tenable Network Security provides, and the operating systems supported by those clients. This table only lists clients that are compatible with the latest version of Tenable Log Correlation Engine.

Client	Operating Systems
Tenable Log Correlation Engine Client for Windows and Linux	<ul style="list-style-type: none">• RHEL/CentOS• Tenable Core• FreeBSD• Debian• OS X• AIX• Solaris• HP-UX• Dragon• Fedora• Ubuntu• SuSE• Windows



Client	Operating Systems
OPSEC Client	<ul style="list-style-type: none">• RHEL/CentOS
Splunk Client	<ul style="list-style-type: none">• RHEL/CentOS
Tenable NetFlow Monitor	<ul style="list-style-type: none">• RHEL/CentOS• Tenable Core
Tenable Network Monitor	<ul style="list-style-type: none">• RHEL/CentOS• Tenable Core
Tenable RDEP Monitor	<ul style="list-style-type: none">• RHEL/CentOS
Tenable SDEE Monitor	<ul style="list-style-type: none">• RHEL/CentOS
Web Query Client	<ul style="list-style-type: none">• RHEL/CentOS
WMI Monitor Client	<ul style="list-style-type: none">• RHEL/CentOS

The Tenable Log Correlation Engine clients can be configured to gather information and events from the following sources:

- Windows Event Logs (collected locally or remotely via WMI)
- Windows/Linux/Unix system and application logs
- Check Point OPSEC events
- Cisco RDEP events
- Cisco SDEE events
- Cisco NetFlow
- Splunk
- Sniffed TCP and UDP network traffic (Tenable Network Monitor)
- Sniffed syslog messages in motion
- File monitoring (Linux, Unix, and Windows)



All data transmitted from Tenable Log Correlation Engine clients to the Tenable Log Correlation Engine server is encrypted using AES-256-CFB.



Tenable Log Correlation Engine Client for Windows

The Tenable Log Correlation Engine Windows Client monitors events, as well as specific log files or directories, for new event data. Tenable provides 32-bit and 64-bit versions of the Tenable Log Correlation Engine Windows Client for Windows Server 2008/2012 R2/2016 and Windows 7/8/10.



System Requirements

Operating System

The Windows Client is compatible with the following operating systems:

- Windows Server 2008/2012, Windows Vista/7/8/10 - 32-bit
- Windows Server 2008/2012 R2/2016, Windows 7/8/10 and Vista - 64-bit

Additional Software

The 5.x Windows Client requires the following software:

- [Microsoft Visual C++ 2015 Redistributable Package, Update 2](#)

Licensing

Tenable Security Center must be licensed for the Tenable Log Correlation Engine Windows Client. For more information, see [Licenses](#) in the Tenable Security Center User Guide.



Install, Configure, and Remove

This section includes the following instructions for installing, configuring, and removing the Log Correlation Engine Windows Client.

- [Download the Tenable Log Correlation Engine Windows Client](#)
- [Install the Tenable Log Correlation Engine Windows Client](#)
- [Install the Log Correlation Engine Windows Client Remotely](#)
- [Configure the Log Correlation Engine Windows Client](#)
- [Remove the Log Correlation Engine Windows Client](#)



Download an Log Correlation Engine Client

For more information, see [Tenable Log Correlation Engine Clients](#).

To download an Log Correlation Engine Client:

1. Access the [Tenable Downloads](#) page.

The **Tenable Downloads** page appears.

2. Click **Log Correlation Engine**.

3. Select the **Tenable Log Correlation Engine** Client you want to download.

The **License Agreement** page appears.

4. Review the Software License Agreement. If you agree to the terms, click the **I Agree** button.

The client package is downloaded.



Install the Tenable Log Correlation Engine Windows Client

In addition to installing the Tenable Log Correlation Engine Windows Client locally, you can also [install the Tenable Log Correlation Engine Windows Client on remote hosts](#).

Before You Begin

[Download the Tenable Log Correlation Engine Windows Client](#).

To install Tenable Log Correlation Engine Windows Client on remote hosts:

1. If you are installing the Tenable Log Correlation Engine Windows Client on a host where User Account Control is enabled, right-click the Tenable Log Correlation Engine Windows Client .msi file and select **Run As Administrator**. Otherwise, double-click the Tenable Log Correlation Engine Windows Client .msi file.

The Tenable Log Correlation Engine Windows Client requires the [Microsoft Visual C++ 2015 Redistributable Package](#). If the package is not installed, an error will appear that instructs you to download and install the package.

The InstallShield Wizard appears.

2. Complete the installation using the InstallShield Wizard.

The Tenable Log Correlation Engine Client is installed.



Install the Log Correlation Engine Windows Client Remotely

The installation of the Log Correlation Engine Windows Client can be accomplished from a command line or script via the execution of `msiexec.exe`. This makes it possible to perform remote installations of Log Correlation Engine Windows Clients for multiple hosts.

To facilitate this process, the option exists to set the client's initial configuration settings at the time of the installation from the same command.

The following table contains a list of PUBLIC properties for the Tenable Log Correlation Engine Windows Client MSI install package. Because all parameters (except Log Correlation Engine server IP address and port) are set using policies on the server, there are only the two options available.

Property	Description
SERVERIP	The IP address or hostname of the Log Correlation Engine server. The maximum length of the hostname is 46 characters. If not specified, the value is set to <i>192.0.2.91</i> .
SERVERPORT	The port used to communicate with the Log Correlation Engine server. The default port is <i>31300</i> .

Caution: Versions of the Log Correlation Engine Windows Client earlier than 4.4 also provided the `SERVERNAME` property. That property is deprecated and should not be used.

Before you begin:

- [Download an Log Correlation Engine Client](#)

To install the Log Correlation Engine Windows Client remotely:

1. Using a script or via the command line, execute the following: "**<Package File>**"
SERVERIP="<Server IP or Hostname>" SERVERPORT=<Port Number>

- **<Package File>** corresponds to the directory location and name of the .msi file. For example, *C:\Users\Administrator\Downloads\<LCE Client Installer>.msi*, where **<LCE Client Installer>** is the file name of the .msi file.



- **<Server IP or Hostname>** corresponds to the IP address or hostname of the Log Correlation Engine server that you want the Log Correlation Engine Windows Client to communicate with. The hostname can be a maximum length of 46 characters.
- **<Port Number>** corresponds to the port used to communicate with the Log Correlation Engine server. Specify an integer between 1 and 65535. The default port is 31300.

If a log file of the installation is desired, **/l** can be used, followed by the path to the log file. For example: `/l C:\Users\Administrator\Documents\lce_client_install.txt /passive /i "C:\Users\Administrators\Downloads\<LCE Client Installer>" SERVERIP="127.0.0.2" SERVERPORT=31300`, where **<LCE Client Installer>** is the file name of the .msi file.

If you want the log file to include all installation information including debug information, instead of **/l**, specify **/lvx***. For example: `/lvx* "install_log.txt" /passive /i "C:\Users\Administrators\Downloads\<LCE Client Installer>" SERVERIP="127.0.0.2" SERVERPORT=31300`, where **<LCE Client Installer>** is the file name of the file.



Configure the Log Correlation Engine Windows Client

If you did not configure the Log Correlation Engine Windows Client [during installation](#), or if you want to modify the configuration, you can configure the client using the command line.

To configure the Log Correlation Engine Windows Client:

1. Via the command line, go to the directory where you installed the Log Correlation Engine Windows Client, then execute the following command: `server_assignment --server-ip "<Server IP or Hostname>" --server-port <Server Port>`
 - **<Server IP or Hostname>** corresponds to the IP address or hostname of the Log Correlation Engine server that you want the Log Correlation Engine Windows Client to communicate with. The hostname can be a maximum length of 46 characters.
 - **<Port Number>** corresponds to the port used to communicate with the Log Correlation Engine server. The default port is 31300.

Note: The default installation location is C:\Program Files\Tenable\LCEClient.

2. Type `net stop "Tenable LCE Client"`

The Log Correlation Engine Client service stops.

3. Type `net start "Tenable LCE Client"`

The Log Correlation Engine Client service starts. The Log Correlation Engine Windows Client is configured.

Note: After the client is configured and authorized by the Log Correlation Engine server, a hidden file named `.lcufh` is created in C:\ProgramData\Tenable\LCE Client. This file contains a cache of process hashes and is used to store hashes that should only be reported once.



Windows Client Policy Configuration Items

The following table lists the configuration items that are valid for the Log Correlation Engine Windows Client policy, and provides a brief description of each item. These configuration items appear in the Client Policy Builder when you create or modify a policy for the Log Correlation Engine Windows Client.

Configuration Item	Description	Valid Values
event-log	<p>The name of a Windows event log to monitor. Each event that appears in event logs monitored by the Log Correlation Engine Windows Client are sent to the Log Correlation Engine server individually. You can specify one or more event logs to monitor.</p> <p>XML Examples:</p> <pre><event-log>Microsoft-Windows-Diagnostics-Performance/Operational</event-log></pre> <pre><event-log>all</event-log></pre> <p>Tip: To locate event providers that you want to include in your policy, use the Windows Event Viewer.</p>	<p>The name of the Windows event log (for example, <i>Application</i>) that you want to monitor, or the value <i>all</i>.</p> <p>If you specify <i>all</i>, in addition to Windows logs, events from Applications and Services logs will also be monitored.</p>
Events to ignore	<p>A provider name that you want the Log Correlation Engine Windows Client to ignore. Additionally, if you do not want to ignore <i>all</i> events from a log provider, you can add specific event IDs for that provider.</p> <p>XML Example:</p> <pre><event-log-filter> <ignore> <provider-name>Microsoft-Windows-Windows</pre>	<p>The provider name must be a valid log provider.</p> <p>The event ID must be an integer. It cannot include any letters or</p>



Configuration Item	Description	Valid Values
	<pre>Defender</provider-name> </ignore> <ignore> <provider-name>Microsoft-Windows- TaskScheduler</provider-name> <event-id>318</event-id> </ignore> <ignore> <provider-name>Microsoft-Windows- WindowsUpdateClient</provider-name> <event-id>41</event-id> <event-id>40</event-id> <event-id>26</event-id> </ignore> </event-log-filter></pre> <div>Tip: To locate event providers that you want the Log Correlation Engine Windows Client to ignore, use the Windows Event Viewer.</div>	symbols.
Monitor text files	<p>The full path and file name of a text file to monitor. Each new line is sent to Log Correlation Engine as a new log.</p> <p>If you want to monitor multiple text files in the same folder, you can specify the following parameters to refine which text files are monitored by the client:</p> <ul style="list-style-type: none">• Location: The full path that contains text files you want to monitor. Each new line in each file is sent to Log Correlation Engine as a new log.• Include: Files in the folder specified for Location will only be monitored if they match the Include pattern. Wildcards are allowed.	Any fully qualified path and file name, including the file extension. It is best practice to escape folder separators with a backslash. For example, C:\\Windows.



Configuration Item	Description	Valid Values
	<ul style="list-style-type: none">Exclude: Files in the folder specified for Location will NOT be monitored if they match the Exclude pattern. Wildcards are allowed.Maximum file size: Files in the folder specified for Location will be deleted once they reach the size specified in this key (in bytes). Optional letters can be post-fixed to change the multiplier (K for kilobytes, M for megabytes, or G for gigabytes). This option was added specifically for Exchange log files, which can grow unbounded. <div>Caution: If you specify a maximum file size, the Tenable Log Correlation Engine Windows Client will attempt to delete files in the folder specified for Location when they go above the maximum file size. Do not use this option if you want to retain the files.</div> <p>XML Examples:</p> <div><pre><flat-file>C:\\Windows\\WindowsUpdate.log</flat-file></pre></div> <div><pre><flat-file> <location>C:\\Windows\\</location> <include>*.log</include> <exclude>iis7.log</exclude> <delete-on-size-bytes>4096K</delete-on-size-bytes> </flat-file></pre></div>	
Monitor binary files	The full path and file name of a non-text file to monitor. If the file changes, the old and new SHA256 checksums	Any absolute path and file



Configuration Item	Description	Valid Values
	<p>are sent as an event to the Log Correlation Engine server. The maximum number of files that can be specified is 63.</p> <p>If multiple files in the same folder are being monitored, you should monitor the folder itself. If you want to monitor multiple files in the same folder, you can specify optional parameters to refine which files are monitored by the client:</p> <ul style="list-style-type: none">• Location: The full path that contains files you want to monitor.• Include: Files in the folder specified for Location will only be monitored if they match the Include pattern. Wildcards are allowed.• Exclude: Files in the folder specified for Location will NOT be monitored if they match the Exclude pattern. Wildcards are allowed. <p>If you want to include or exclude directories in the same folder, you can specify optional parameters to refine which files are monitored by the client:</p> <ul style="list-style-type: none">• Include-dir: Included directory path for monitoring files. Wildcards are allowed.• Exclude-dir: Excluded directory path for monitoring files. Wildcards are allowed. <p>XML Example:</p> <pre><monitor-file>C:\\Windows\\notepad.exe</monitor-file> <monitor-file></pre>	<p>name, including the file extension. It is best practice to escape folder separators with a backslash. For example, <i>C:\\Windows</i>.</p>



Configuration Item	Description	Valid Values
	<pre><location>C:\\Windows\\</location> <include>*.exe</include> <exclude>explorer.exe</exclude> <include- dir>C:\\Windows\\System32\\</include-dir> <exclude-dir>C:\\Windows\\debug\\</exclude- dir> </monitor-file></pre>	
monitor-subdirectories	<p>Whether to monitor files in subdirectories of the folder specified for Location for Monitor binary files, if those files match the specified pattern.</p> <p>If set to 1, monitoring an extensive folder structure (such as C:\\Windows) with no include or exclude filters may impact performance.</p> <p>XML Example:</p> <pre><monitor-subdirectories>1</monitor- subdirectories></pre>	0 (off) or 1 (on)
Monitor wait seconds	<p>The number of seconds to wait before monitoring files. The default is 5 seconds.</p> <p>XML Example:</p> <pre><monitor-wait-seconds>10</monitor-wait-seconds></pre>	An integer greater than 0.
Tail subdirectories	<p>Whether to monitor files in subdirectories of the folder specified for Location for Monitor text files, if those files match the specified pattern.</p> <p>If set to 1, monitoring an extensive folder structure (such as C:\\Windows) with no include or exclude filters</p>	0 (off) or 1 (on)



Configuration Item	Description	Valid Values
	<p>may impact performance.</p> <p>XML Example:</p> <pre><tail-subdirectories>1</tail-subdirectories></pre>	
Seconds between scans of logs and text files	<p>The number of seconds between scanning logs monitored by the Log Correlation Engine Windows Client.</p> <p>XML Example:</p> <pre><interval-log-seconds>30</interval-log-seconds></pre>	An integer greater than 0.
monitor-wait-seconds	<div>Caution: This option is not available for the Log Correlation Engine Windows Client versions 4.4 and later.</div>	No valid values
Send new events only	<p>Whether to only send new events. If set to 0, all data in all monitored logs will be sent to the Log Correlation Engine server every time the client is restarted or when the policy changes.</p> <p>XML Example:</p> <pre><send-new-events-only>1</send-new-events-only></pre>	0 (off) or 1 (on)
Monitor config	<div>Caution: This option is not available for the Log Correlation Engine Windows Client versions 4.4 and later.</div>	No valid values
Report unknown processes	<p>If enabled, the Log Correlation Engine Windows Client will send an LCE_Client_Detected_Unknown_Process event for each unknown process on the monitored host. This event is sent once for each unknown process detected.</p>	<p>0 (off), 1, or 2</p> <ul style="list-style-type: none">1: A list of LCE_Client_



Configuration Item	Description	Valid Values
	<p>XML Example:</p> <pre><report-unknown-processes>2</report-unknown-processes></pre>	<p>Detected_Unknown_Process events will be sent only once, and subsequently only newly-encountered unknown DLLs and EXEs will be reported.</p> <ul style="list-style-type: none">• 2: The list of reported unknown processes will be cleared every time the client is restarted or a new policy is received.



Configuration Item	Description	Valid Values
		All existing unknown DLLs and EXEs will be sent to the Tenable Log Correlation Engine server again.
Remote host to monitor	<p>Using the following parameters, specifies a remote host to monitor:</p> <ul style="list-style-type: none">• IP address: The IP address of the host that you want to monitor.• Namespace: The namespace of the WMI classes being monitored, usually <i>root\cimv2</i>.• Domain: The domain of the remote host to monitor.• Username: The user name of the account on the remote machine that should be used for monitoring.• Password: The corresponding password for the specified user name.• File paths to monitor: One or more fully qualified paths with file name and extension that you want to monitor on the remote host.	All parameters require values.



Configuration Item	Description	Valid Values
	<p>XML Example:</p> <pre><Host> <ip>192.0.2.10</ip> <namespace>root\cimv2</namespace> <domain>?</domain> <username>corpnetAdmin</username> <password>argus\$12</password> <logfilename>C:\\Windows\\WindowsUpdate.log- </logfilename> </Host></pre>	
Info	<p>Enable or disable info-level logging in Ice_client.log (the Log Correlation Engine client debugging log).</p> <p>XML Example:</p> <pre><info>0</info></pre>	0 (off) or 1 (on)
Verbose	<p>Enable or disable verbose logging in Ice_client.log (the Log Correlation Engine client debugging log).</p> <p>XML Example:</p> <pre><verbose>0</verbose></pre>	0 (off), 1, or 2 <ul style="list-style-type: none">1:2: Additional debugging information.
Debug	<p>Whether to enable debugging messages in Ice_client.log (the Log Correlation Engine Windows Client log). If <debug>1</debug> is present in the policy, debugging messages are enabled. It is recommended you only enable debugging if directed to do so by Tenable Network Security.</p>	0 (off) or 1 (on)



Configuration Item	Description	Valid Values
	<p>XML Example:</p> <pre><debug>0</debug></pre>	
Client heartbeat frequency	<p>The number of seconds between each client heartbeat message to the Log Correlation Engine server. If set to 0, the client will not send heartbeats.</p> <p>XML Example:</p> <pre><heartbeat-frequency>600</heartbeat-frequency></pre>	An integer
Client statistics frequency	<p>The number of minutes between each client host performance statistics report (CPU, Disk Space, and Physical Memory) to the Log Correlation Engine server. If set to 0, client statistics will not be sent.</p> <p>XML Example:</p> <pre><statistics-frequency>60</statistics-frequency></pre>	An integer
Compress events	<p>Whether client will compress log data prior to sending it to the Log Correlation Engine server in order to save bandwidth. Recommended except when debugging. If set to 0, events will not be compressed.</p> <p>XML Example:</p> <pre><compress-events>1</compress-events></pre>	0 (off) or 1 (on)
Compression level	<p>Compression level to use when compressing events for transmission across network using zlib, set on a scale from 1 to 9. 1 provides the least amount of compression, resulting in minimum CPU usage and minimum</p>	An integer from 1 to 9.



Configuration Item	Description	Valid Values
	<p>bandwidth savings; 9 maximizes compression, resulting in increased CPU usage and maximum bandwidth savings. Ignored unless compression is enabled.</p> <p>XML Example:</p> <pre><compression-level>5</compression-level></pre>	
Minimum compression ratio	<p>Defines the minimum acceptable savings ratio for event data being transmitted across the network, in terms of (bytes total) / (bytes compressed). If the client determines a savings ratio of less than this value, then event data will not be compressed before sending. This reduces the effort on the Log Correlation Engine Server decompressing event data when compression benefits are minimal. Ignored unless compression is enabled.</p> <p>XML Example:</p> <pre><minimum-compression-ratio>1.5</minimum-compression-ratio></pre>	A decimal number.
Minimum compression input size	<p>The minimum number of bytes a packet must have to be compressed. Ignored unless compression is enabled.</p> <p>XML Example:</p> <pre><minimum-compression-input-size>2048</minimum-compression-input-size></pre>	An integer greater than 0.
Event queue timeout	<p>Maximum number of seconds between event messages the client sends to the Tenable Log Correlation Engine server.</p> <p>XML Example:</p>	An integer greater than 0.



Configuration Item	Description	Valid Values
	<pre><event-queue-timeout>30</event-queue-timeout></pre>	
Malware scan period	<p>This option specifies the interval (in seconds) that the Log Correlation Engine Windows Client will scan running processes, and monitored directories.</p> <p>XML Example:</p> <pre><malware-scan-frequency>600</malware-scan-frequency></pre>	An integer greater than 0.
Whitelist hashes	<p>MD5 file hashes that will be ignored by Log Correlation Engine Windows Client that may otherwise be considered malware.</p> <p>XML Example:</p> <pre><whitelist-hashes>8d1ae0900d461fd593b4daf67ee72e00</whitelist-hashes></pre>	An MD5 hash.
Custom malware hashes	<p>MD5 file hashes that will be identified as malware by the Log Correlation Engine Windows Client if detected.</p> <p>XML Example:</p> <pre><custom-malware-hashes>e1112134b6dcc8bed54e0e34d8ac272795e73d74- </custom-malware-hashes></pre>	An MD5 hash.



Remove the Log Correlation Engine Windows Client

The Log Correlation Engine Windows Client can be removed in three ways:

- [Using the original .msi file](#)
- [Using the command line](#)
- Using the Control Panel for your version of Windows

Note: This method will vary based on your operating system. If you are unsure how to remove a program using the Control Panel, consult the documentation for your operating system.

To remove The Log Correlation Engine Windows Client using the Log Correlation Engine Windows Client .msi File

1. If you are removing the Log Correlation Engine Windows Client from a host where User Account Control is enabled, right-click the Log Correlation Engine Windows Client .msi file and select **Run As Administrator**. Otherwise, double-click the Log Correlation Engine Windows Client .msi file.

The InstallShield Wizard appears.

On the **Program Maintenance** screen, you are prompted to **Modify**, **Repair**, or **Remove** the installation.

2. Select **Remove**, and then click the **Next** button.

The **Remove the Program** screen appears. You are prompted to remove all files in program data folders. By default, the **Remove all files in program data folders** check box is selected.

3. If you do not want to remove local files that were created by the Log Correlation Engine Windows Client, clear the **Remove all files in program data folders** check box.
4. Click the **Next** button.

The **Files in Use** screen appears. The Tenable Log Correlation Engine Client service must be stopped in order for the removal to complete successfully. By default, the Tenable Log Correlation Engine Client service will be stopped.



5. If you do not want to stop the Tenable Log Correlation Engine Client service, select **Do not close applications**. Your computer will need to be restarted before the removal process is completed.
6. Click **OK**, and then complete the InstallShield Wizard.

The Log Correlation Engine Windows Client is removed.

To remove the Log Correlation Engine Windows Client using the CLI

1. Via the command line, execute the following: `/uninstall "<Package File>"`
 - **<Package File>** corresponds to the directory location and name of the .msi file. For example, *C:\Users\Administrator\Downloads\lce_client-4.4.0-windows_2008_x64.msi*. The exact package name will vary.



Tenable Log Correlation Engine Windows Client Features

The Tenable Log Correlation Engine Windows Client is used to monitor events from many different channels on supported Windows platforms, including logs created by applications, and any Windows event logs. Additionally, the client can be configured to monitor text and binary files on a host, report on MD5 hash changes, monitor unknown processes, and scan for malware. Remote hosts can also be monitored.

Event and Text File Monitoring

Whenever a new event appears in a monitored Windows event log, the event is transmitted to the Tenable Log Correlation Engine server for normalization. In the case of monitored text files, each new line is transmitted. After the Tenable Log Correlation Engine server normalizes the event data, the data can be visualized using Tenable Security Center. The Tenable Log Correlation Engine Windows Client can process files of all common encoding types, including UTF-8 and UTF-16.

Binary File and Unknown Process Monitoring

When a binary or executable file is monitored, if the MD5 checksum of the file changes, the old and new MD5 hashes are transmitted to the Tenable Log Correlation Engine server as an event. When unknown processes are monitored, you can configure the Tenable Log Correlation Engine Windows Client to report all unknown processes that are detected every time the client is restarted, or to report only newly-identified unknown processes.

Malware Scan

When the Tenable Log Correlation Engine Windows Client is configured to scan for malware, it will check the MD5 checksums of all running processes, as well as any binary file that the Tenable Log Correlation Engine Windows Client is monitoring, and compare the checksums to the Tenable database of known malware. Any processes or files that are identified as malware will be reported to the Tenable Log Correlation Engine server as events. When malware scanning is enabled, the Tenable Log Correlation Engine Windows Client will use DNS queries to compare the MD5 checksums.

Configure the Windows Client Policy

Using the [Client Policy Builder](#), you can create and modify policies for your Tenable Log Correlation Engine Windows Client. The following steps are performed via the web interface on the Tenable Log Correlation Engine server that you configured your Tenable Log Correlation Engine Windows Client to communicate with.

The screenshot displays the LCE (Log Correlation Engine) web interface. The top navigation bar includes links for Health and Status, Configuration, Clients, Policies, and Users. The current page is titled "default_windows_tenableclient.lcp - Tenable Client, Windows". The interface is split into two main sections: "Basic" and "Advanced".

Basic Section:

- Event log:** A dropdown menu showing "Application", "Security", and "System".
- Events to ignore:** A button to toggle this setting.
- Monitor text files:** A button to toggle this setting.
- Monitor binary files:** A button to toggle this setting.
- File paths:** A list of file paths to monitor, including C:\MSDOS.SYS, C:\IO.SYS, C:\config.sys, C:\BOOTSECT.BAK, C:\autoexec.bat, C:\Program Files\Tenable\LCEClient, C:\Windows, C:\Windows\System32, and C:\Windows\system.
- Monitor subdirectories:** A checkbox.
- Tail subdirectories:** A checkbox.
- Seconds between scans of logs and text files:** A text input field with the value "60".
- Interval monitor:** A text input field with the value "No value defined."

Advanced Section:

The Advanced section displays an XML configuration file. The XML content is as follows:

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<!-- Created with LCE web policy editor by user admin -->
<options xmlns:xi="http://www.w3.org/2003/XInclude">
  <event-log>Application</event-log>
  <event-log>Security</event-log>
  <event-log>System</event-log>
  <monitor-file>C:\MSDOS.SYS</monitor-file>
  <monitor-file>C:\IO.SYS</monitor-file>
  <monitor-file>C:\config.sys</monitor-file>
  <monitor-file>C:\BOOTSECT.BAK</monitor-file>
  <monitor-file>C:\autoexec.bat</monitor-file>
  <monitor-file>C:\Program Files\Tenable\LCEClient</monitor-file>
  <monitor-file>C:\Windows</monitor-file>
  <monitor-file>C:\Windows\System32</monitor-file>
  <monitor-file>C:\Windows\system</monitor-file>
  <monitor-subdirectories>0</monitor-subdirectories>
  <tail-subdirectories>0</tail-subdirectories>
  <interval-log-seconds>60</interval-log-seconds>
  <send-new-events-only>1</send-new-events-only>
  <monitor-config>0</monitor-config>
  <info>0</info>
  <verbose>0</verbose>
  <debug>1</debug>
  <statistics-frequency>60</statistics-frequency>
  <heartbeat-frequency>300</heartbeat-frequency>
  <compress-events>1</compress-events>
</options>
```

To configure the Windows Client Policy:

1. Using the Client Policy Builder, [create a policy for your Tenable Log Correlation Engine Windows Client](#). This documentation includes a list of [valid configuration items for the client policy](#).
2. [Assign the policy to the Tenable Log Correlation Engine Windows Client](#).



Tenable Log Correlation Engine Client for Linux

The documentation for the most recent version of the Tenable Log Correlation Engine Client for Linux is currently available starting on page 18 of the following document:

http://static.tenable.com/prod_docs/LCE_4.2_clients.pdf



OPSEC Client

The documentation for the OPSEC Client is currently available here:

https://docs.tenable.com/other/lce/LCE_4.5.0_OPSEC_Client_Guide.pdf



Get Started with the Tenable Log Correlation Engine Splunk Client

Tenable Log Correlation Engine unifies vulnerability collection and event analysis data through Tenable Security Center, which provides easy-to-use dashboards to display multiple data points in a centralized view. Organizations that choose to send Splunk logs to the Tenable Log Correlation Engine have a unique advantage in that Splunk data is normalized by Tenable Log Correlation Engine and can be included for automatic anomaly detection, discovering assets, and additional vulnerability information including botnet and malware detection.

The Tenable Log Correlation Engine Splunk Client forwards data that Splunk collects to the Tenable Log Correlation Engine server. Once the data reaches the Tenable Log Correlation Engine server, the data is reviewed and normalized so it can be queried in Tenable Security Center. The scope of this client can vary depending on what data is being forwarded from Splunk to the Tenable Log Correlation Engine Splunk Client.

Caution: The Tenable Log Correlation Engine Splunk Client can process a maximum of 500 logs per second. Processing more than 500 logs per second can result in a loss of data. This is an absolute limit and *cannot* be increased by improving the system hardware.



Install, Configure, and Remove

This section includes the following instructions for installing, configuring, and removing the Log Correlation Engine Splunk Client. With the exception of downloading the Splunk Client, the following procedures must be performed on the command line.

- [Download the Tenable Log Correlation Engine Splunk Client](#)
- [Install the Log Correlation Engine Splunk Client](#)
- [Configure the Log Correlation Engine Splunk Client](#)
- [Remove the Log Correlation Engine Splunk Client](#)



Install the Log Correlation Engine Splunk Client

To install the Tenable Log Correlation Engine Splunk Client:

Note: All shell commands need to be executed by a user with root privileges.

1. Copy the downloaded client package to the host where it will be installed. The Log Correlation Engine Splunk Client can be installed directly on a Splunk server.
2. Verify the MD5 checksum of the client package against the MD5 checksum found in the [release notes](#).

Example:

```
# md5sum lce_splunk-4.6.0-el6.x86_64.rpm
da9f07886a693fb69cba1dbd5c3eba31  lce_splunk-4.6.0-el6.x86_64.rpm
```

3. To initiate the installation, type the following command:

rpm -ivh <package name>, where **<package name>** is the name of the client package.

Example:

```
# rpm -ivh lce_splunk-4.6.0-el6.x86_64.rpm
Preparing...      ##### [100%]
1:lce_splunk      ##### [100%]
Checking for existence of TAG file at /etc/tenable_tag ...
Writing TAG to /etc/tenable_tag ...
```



Configure the Log Correlation Engine Splunk Client

Note: All shell commands need to be executed by a user with root privileges.

To configure the Splunk Client, you can execute the **set-server-ip.sh** script and include the Log Correlation Engine Server IP address and port number as arguments, or execute the script and, when prompted, enter the IP address and port number individually.

Finally, you will need to [authorize the Tenable Log Correlation Engine Splunk Client](#).

To execute the script using arguments:

1. Type **/opt/lce_splunk/set-server-ip.sh <IP> <Port>**, where *<IP>* is the IP address of an Log Correlation Engine Server and *<Port>* is the port number assigned to the server. By default, the port number is *31300*.

The Log Correlation Engine Server IP address and port number are updated, and the Log Correlation Engine Splunk Client daemon is restarted.

Example:

```
# /opt/lce_splunk/set-server-ip.sh 192.168.22.11 31300
Updating LCE Server IP from 192.0.2.66 to 192.0.2...
Updating LCE Server Port from 31300 to 31300...
Done
Stopping LCE Splunk Client daemon                [ OK ]
Starting LCE Splunk Client daemon                  [ OK ]
```

To execute the script without arguments:

1. Type **/opt/lce_splunk/set-server-ip.sh**

You are prompted to enter the Log Correlation Engine Server IP address or hostname.

2. Type the IP address or hostname of an Log Correlation Engine server.

You are prompted to enter the Log Correlation Engine server port.

3. Type the port number assigned to the server for Log Correlation Engine client communication. By default, the port number is *31300*.



The Log Correlation Engine Server IP address and port number are updated, and the Log Correlation Engine Splunk Client daemon is restarted.

Example:

```
# /opt/lce_splunk/set-server-ip.sh

Enter the new desired LCE server IP or hostname.
>>
192.168.22.11

Enter the new desired LCE server port [31300].
>>
31300
Updating LCE Server IP from 203.0.113.1 to 192.168.22.11...
Updating LCE Server Port from 31300 to 31300...
Done
Stopping LCE Splunk Client daemon           [ OK ]
Starting LCE Splunk Client daemon           [ OK ]
```



Remove the Log Correlation Engine Splunk Client

Note: All shell commands need to be executed by a user with root privileges.

To remove the Log Correlation Engine Splunk Client:

1. To query the rpm database to obtain the name of the currently installed package, type **rpm -qa |grep lce_**.

Example:

```
# rpm -qa |grep lce_  
lce_splunk-4.6.0-el6.x86_64.rpm
```

2. Type **rpm -e lce_splunk**.

The Splunk Client package is removed.

Example:

```
# rpm -e lce_splunk  
warning: /opt/lce_splunk/server_assignment.xml saved as /opt/lce_splunk/server_  
assignment.xml.rpm.save
```

3. Optionally, type **rm -rf /opt/lce_splunk/** to remove the Splunk Client install directory. Configuration and log files will remain unless the directory is removed.

An additional file, */etc/tenable_tag*, will be installed with the Splunk Client if it does not already exist. This file contains a UUID that tracks all events related to the endpoint on which the client is installed. This file should *only* be removed if no other Tenable products are in use, and no others will be installed on the endpoint in the future.



Tenable Log Correlation Engine Splunk Client Features

The Tenable Log Correlation Engine Splunk Client provides you a way to move data from your Splunk instances into Tenable Security Center by way of Tenable Log Correlation Engine. Tenable Security Center is then used to comprehensively [visualize the data from Splunk](#).

After the Tenable Log Correlation Engine Splunk Client is installed and configured, you configure the Splunk Indexer to forward data to the Tenable Log Correlation Engine Splunk Client. The client then sends that data to the Tenable Log Correlation Engine server, which normalizes it. Finally, that normalized data is sent to Tenable Security Center.



Data Comparison

An example of the data shown in Splunk is shown below. The example shown contains search results for a Cisco ASA firewall. The exact search used narrowed the results to *sourcetype=syslog*, and matched the text string *%ASA*.

The screenshot shows the Splunk Search & Reporting interface. The search bar contains the query `sourcetype=syslog %ASA`. Below the search bar, it indicates 32,664 events. The results are displayed in a table with columns for Time, Event, and Source. The table shows a list of events from April 1, 2014, at 20:11:31. The events include various syslog messages from a Cisco ASA firewall, such as 'SASA-5-304001: 10.31.104.129 Accessed URL 74.125.226.229: http://clients1.google.com/generate_204' and 'SASA-6-305011: Built dynamic TCP translation from inside: 10.31.104.129/59373 to outside: 173.162.234.193/59373'.


Time	Event	Source
4/1/14 8:11:31.000 PM	SASA-5-304001: 10.31.104.129 Accessed URL 74.125.226.229: http://clients1.google.com/generate_204	host = 10.31.254.254 source = udp/514 sourcetype = syslog
4/1/14 8:11:31.000 PM	SASA-6-305011: Built dynamic TCP translation from inside: 10.31.104.129/59373 to outside: 173.162.234.193/59373	host = 10.31.254.254 source = udp/514 sourcetype = syslog
4/1/14 8:11:31.000 PM	SASA-6-305011: Built dynamic TCP translation from inside: 10.31.104.129/59372 to outside: 173.162.234.193/59372	host = 10.31.254.254 source = udp/514 sourcetype = syslog
4/1/14 8:11:31.000 PM	SASA-6-305011: Built dynamic UDP translation from inside: 10.31.100.10/50403 to outside: 173.162.234.193/50403	host = 10.31.254.254 source = udp/514 sourcetype = syslog
4/1/14 8:11:31.000 PM	SASA-4-401004: Shunned packet: 10.31.104.140 ==> 157.56.53.41 on interface inside	host = 10.31.254.254 source = udp/514 sourcetype = syslog
4/1/14 8:11:31.000 PM	SASA-6-305011: Built dynamic UDP translation from inside: 10.31.100.10/49589 to outside: 173.162.234.193/49589	host = 10.31.254.254 source = udp/514 sourcetype = syslog
4/1/14 8:11:31.000 PM	SASA-5-304001: 10.31.104.129 Accessed URL 23.3.106.51: http://fpdownload2.macromedia.com/get/flashplayer/update/current/xml/version_en_mac_p1.xml	host = 10.31.254.254 source = udp/514 sourcetype = syslog
4/1/14 8:11:31.000 PM	SASA-6-305011: Built dynamic TCP translation from inside: 10.31.104.129/59371 to outside: 173.162.234.193/59371	host = 10.31.254.254 source = udp/514 sourcetype = syslog
4/1/14 8:11:31.000 PM	SASA-6-305011: Built dynamic UDP translation from inside: 10.31.100.10/69051 to outside: 173.162.234.193/69051	host = 10.31.254.254 source = udp/514 sourcetype = syslog
4/1/14 8:11:31.000 PM	SASA-6-305011: Built dynamic TCP translation from inside: 10.31.104.129/59370 to outside: 173.162.234.193/59370	host = 10.31.254.254 source = udp/514 sourcetype = syslog
4/1/14 8:11:31.000 PM	SASA-5-304001: 10.31.104.129 Accessed URL 74.125.226.165: http://s.ytimg.com/yts/swf/masthead_child-vf13RM06_swf	host = 10.31.254.254 source = udp/514 sourcetype = syslog
4/1/14 8:11:31.000 PM	SASA-5-304001: 10.31.104.129 Accessed URL 74.125.226.165: http://s.ytimg.com/yts/swfbin/player-vf1QLTy25/watch_as3.swf	host = 10.31.254.254 source = udp/514 sourcetype = syslog

The same type of log information is available in Tenable Security Center. When a user logs into Tenable Security Center, there can be multiple dashboards available that display pertinent information for that user. It is possible to set a specific collection of dashboards as the default view in Tenable Security Center. Examples of dashboards that can be created for events that are collected by the Tenable Log Correlation Engine Splunk client.

The **Splunk Events** dashboard in the previous example contains a component named **NormalizedEvent Types Collected by Splunk**. Click [▶](#) beside that component to view all the information available.

The **NormalizedEvent Types Collected by Splunk** component on the **Splunk Events** dashboard includes the Cisco ASA Firewall events and all event types in a normalized format that is easy to interpret. There are several views that you can select on the **Event Analysis** page that can be displayed by selecting **Normalized Event Summary**. A view similar to that in Splunk can be seen by clicking the **Raw Syslog Events** link.



It is also possible to filter the **Normalized Event Summary** along with any other summary view by clicking  at the top left of the window. The text string %ASA used in the Splunk search could be typed in the **Syslog Text** box.



Configure Splunk

This section describes the steps necessary to receive data from Splunk with the Tenable Log Correlation Engine Splunk Client.

- [Configure the Splunk Indexer to forward data to the Tenable Log Correlation Engine Splunk Client.](#)
- [Configure and assign the client policy for the Tenable Log Correlation Engine Splunk Client.](#)



Configure Splunk to Forward Data

The following procedure is performed on the Splunk Indexer that you want to forward data to the Tenable Log Correlation Engine Splunk Client.

To configure the Splunk Client to Forward Data:

1. Access [Splunk Web](#) as a user with Administrator privileges.
2. At the top of the Splunk Web interface, [click **Settings**, and then click **Forwarding and receiving**](#).

The **Forwarding and receiving** page appears.

3. In the **Configure forwarding** row, in the **Actions** column, click the **Add new** link.

The **Add new** page appears.

4. In the **Host** box, type the IP address of the Tenable Log Correlation Engine Splunk Client host, and then click the **Save** button.

The IP address is saved. On the Splunk Web interface, the IP address appears on the **Forward data** page.

5. Access the Splunk Indexer as the root user.
6. Edit the **outputs.conf** file, usually located at `/opt/splunk/etc/system/local/outputs.conf`. The lines you must add appear in bold.

```
[tcpout]
defaultGroup = default
disabled = 0
indexAndForward = 1
[tcpout-server://LCE_IP_OR_Hostname:9800]
[tcpout:default]
disabled = 0
server = LCE_IP_OR_Hostname:9800
sendCookedData = false
```

7. Save the file, and then restart the Splunk services.

Data will now be forwarded to the Tenable Log Correlation Engine Splunk Client.



Configure the Splunk Client Policy

Using the [Client Policy Builder](#), you can create and modify policies for your Tenable Log Correlation Engine Splunk Client. The following steps are performed via the web interface on the Tenable Log Correlation Engine server that you configured your Tenable Log Correlation Engine Splunk Client to communicate with.

Caution: The Tenable Log Correlation Engine Splunk Client can process a maximum of 500 logs per second. Processing more than 500 logs per second can result in a loss of data. This is an absolute limit and *cannot* be increased by improving the system hardware.

To configure the Splunk Client:

1. Using the Client Policy Builder, [create a policy for your Tenable Log Correlation Engine Splunk Client](#). This documentation includes a list of [valid configuration items for the client policy](#).

Note: The Tenable Log Correlation Engine Splunk Client policy requires at least one IP address for a Splunk server. If no IP addresses are provided, the client will not open the Listen port.

In order for the Splunk Client to function, you will need to edit the Client policy, include the required syntax noted below, and specify your Splunk server.

XML Example:

```
<splunk-server>192.0.2.10</splunk-server>
```

2. [Assign the policy to the Tenable Log Correlation Engine Splunk Client](#).



Additional Resources

This section contains the following additional resources:

- [Splunk Client Policy Configuration Items](#)



Splunk Client Policy Configuration Items

In the Client Policy Builder, the following configuration items appear for the Tenable Log Correlation Engine Splunk Client.

The following table lists the configuration items that are valid for the Tenable Log Correlation Engine Splunk Client, and provides a brief description of each.

Configuration Item	Description	Valid Values
Splunk server	<p>The IP addresses of one or more Splunk servers that are sending data to the Tenable Log Correlation Engine Splunk Client.</p> <div>Note: The Tenable Log Correlation Engine Splunk Client requires at least one IP address to be entered in order to receive data. If no Splunk servers are added, the Tenable Log Correlation Engine Splunk Client will not open the Listen port.</div> <p>In order for the Splunk Client to function, you will need to edit the Client policy, include the required syntax noted below, and specify your Splunk server.</p> <p>XML Example:</p> <pre><splunk-server>192.0.2.10</splunk-server></pre>	One IP address per entry.
Listen port	<p>The port to which the Splunk servers are sending data.</p> <p>XML Example:</p> <pre><listen-port>8000</listen-port></pre>	An integer from 1024 to 65535. Privileged ports (lower than 1024) are not valid for this configuration item.
Syslog server	The IP address or hostname and port number of the syslog server that you want the Tenable Log	<IP or Hostname>:<Port



Configuration Item	Description	Valid Values
	<p>Correlation Engine Splunk Client to forward events to in addition to the Tenable Log Correlation Engine server.</p> <p>XML Examples:</p> <pre><syslog-server>192.0.2.10:8000</syslog-server></pre> <pre><syslog-server>corpnet8557:8000</syslog-server></pre>	<p>Number>, where</p> <ul style="list-style-type: none">• <IP or Hostname> is an IP address, or a hostname that is a maximum length of 46 characters.• <Port Number> is an integer from 1 to 65535.
Delimiter	<p>The custom delimiters that you want to apply to parse events in Splunk logs. You can include multiple Delimiter entries in your policy.</p> <div>Note: By default, the policy includes the delimiter for Windows multiline logs. This delimiter is not required by the policy.</div> <p>XML Example:</p> <pre><delimiters> <delimiter> <start>\d{1,2}/\d{2}/\d{4} \d{2}:\d{2}:\d{2} (A P)M</start> <end>[^\r]\n</end> </delimiter> </delimiters></pre>	See Delimiters
Log directory	Directory containing files, named according to the	A path to an existing



Configuration Item	Description	Valid Values
	<p>date, that contain Tenable Log Correlation Engine Splunk Client log messages.</p> <p>XML Example:</p> <pre><log-directory></log-directory></pre>	directory.
Client heartbeat frequency	<p>Caution: This configuration item is deprecated for versions 4.6 and later of the Tenable Log Correlation Engine Splunk Client. Client heartbeat period should be used instead.</p> <p>XML Example:</p> <pre><heartbeat-frequency>600</heartbeat-frequency></pre>	No valid values.
Client heartbeat period	<p>The number of seconds between each client heartbeat message to the Tenable Log Correlation Engine server. If not used or set to 0, the client will not send heartbeats.</p> <p>XML Example:</p> <pre><heartbeat-period>600</heartbeat-period></pre>	An integer.
Client statistics frequency	<p>Caution: This configuration item is deprecated for versions 4.6 and later of the Tenable Log Correlation Engine Splunk Client. Client statistics period should be used instead.</p> <p>XML Example:</p> <pre><statistics-frequency>60</statistics-</pre>	No valid values.



Configuration Item	Description	Valid Values
	<pre>frequency></pre>	
Client statistics period	<p>The number of minutes between each client host performance statistics report (CPU, Disk Space, and Physical Memory) to the Tenable Log Correlation Engine server. If not used or set to 0, client statistics will not be sent.</p> <p>XML Example:</p> <pre><statistics-period>60</statistics-period></pre>	An integer.
Compress events	<p>Whether client will compress log data prior to sending it to the Tenable Log Correlation Engine server in order to save bandwidth. Recommended except when debugging. If set to 0, events will not be compressed.</p> <p>XML Example:</p> <pre><compress-events>1</compress-events></pre>	0 (off) or 1 (on)
Compression level	<p>Compression level to use when compressing events for transmission across network using zlib, set on a scale from 1 to 9. 1 provides the least amount of compression, resulting in minimum CPU usage and minimum bandwidth savings; 9 maximizes compression, resulting in increased CPU usage and maximum bandwidth savings. Ignored unless compression is enabled.</p> <p>XML Example:</p>	An integer from 1 to 9.



Configuration Item	Description	Valid Values
	<pre><compression-level>5</compression-level></pre>	
Minimum compression ratio	<p>Defines the minimum acceptable savings ratio for event data being transmitted across the network, in terms of (bytes total) / (bytes compressed). If the client determines a savings ratio of less than this value, then event data will not be compressed before sending. This reduces the effort on the Tenable Log Correlation Engine Server decompressing event data when compression benefits are minimal. Ignored unless compression is enabled.</p> <p>XML Example:</p> <pre><minimum-compression-ratio>1.5</minimum-compression-ratio></pre>	A decimal number.
Minimum compression input size	<p>The minimum number of bytes a packet must have to be compressed. Ignored unless compression is enabled.</p> <p>XML Example:</p> <pre><minimum-compression-input-size>2048</minimum-compression-input-size></pre>	An integer greater than 0.
Debug level	<p>Controls the debugging information that is logged.</p> <p>XML Example:</p> <pre><debug-level>NONE</debug-level></pre>	<p>One of the following values:</p> <ul style="list-style-type: none">• NONE• VERBOSE• INFO



Configuration Item	Description	Valid Values
		<ul style="list-style-type: none">• WARN• ERROR
Event queue timeout	<p>Maximum number of seconds between event messages the client sends to the Tenable Log Correlation Engine server.</p> <p>XML Example:</p> <pre><event-queue-timeout>30</event-queue-timeout></pre>	An integer greater than 0.
Local IP net	<p>If a host has multiple network connections, allows you to specify which network to use. If not set or if the CIDR does not match any networks, the client will use the first network connection detected.</p> <p>XML Example:</p> <pre><local-ip-net>192.0.2.0/8</local-ip-net></pre>	A CIDR.
Event file	<p>Path to file for receiving events. Relative paths are interpreted to start at the client's installation directory.</p> <p>XML Example:</p> <pre><write-events-to-file></write-events-to-file></pre>	A path to an existing file.
Write events to standard output	<p>Whether to write events to standard output (stdout). Any event picked up by the Tenable Log Correlation Engine Splunk Client will have the raw</p>	0 (off) or 1 (on)



Configuration Item	Description	Valid Values
	<p>log printed to the stdout of the client, the default being a terminal session, before the client sends it to the Tenable Log Correlation Engine server to be processed. This configuration item is useful for debugging and troubleshooting.</p> <p>XML Example:</p> <pre><write-events-to-stdout>0</write-events-to-stdout></pre>	



Delimiters

Depending on the needs of your organization and the types of logs coming from your Splunk server, you may want to implement custom delimiters in the client policy for your Tenable Log Correlation Engine Splunk Client.

By default, the Tenable Log Correlation Engine Splunk Client parses each line in a log as an event. Because not all logs capture events on a single line, delimiters can be implemented that allow the Tenable Log Correlation Engine Splunk Client to capture multiple lines and parse them as a single event. If a log had more than one event stored on a single line, you can implement delimiters that allow the Tenable Log Correlation Engine Splunk Client to parse multiple events from a single line.

Caution: Delimiters should only be implemented by advanced users with an understanding of ECMA regular expression grammar.

The Tenable Log Correlation Engine Splunk Client policy can include zero or more delimiters. Delimiters are not required. In the case that delimiters are included in the policy but do not match in a log, the Tenable Log Correlation Engine Splunk Client uses the default behavior of parsing each line in a log as an event.

Because logs from Splunk may come from many different sources, you can include multiple delimiters in your Tenable Log Correlation Engine Splunk Client policy to account for the different methods of logging.

There are several considerations when implementing client policy delimiters:

- In the client policy, delimiters consist of Start and End expressions. The Start and End expressions are used to identify the starting and ending strings of the events you want to capture.

For example, the default Start expression that appears in the policy is `\d{1,2}/\d{2}/\d{4}\d{2}:\d{2}:\d{2} (A|P)M`, which will match an event that starts with a value such as `06/15/2016 05:23:06 AM`. The End expression is `[^\r]\n`, which matches a newline that is not preceded by a carriage return. This delimiter allows the Tenable Log Correlation Engine Splunk Client to capture multiple-line events from Windows logs.

- Delimiters should be entered in order of priority. In the client policy, delimiters will be tested in the order they appear. If a delimiter is found to be valid for a log (i. e., the Start expression matches), no subsequent delimiters will be applied. Only one delimiter will be applied to a log.



- Delimiters must be entered using ECMA regular expression grammar.
- If a delimiter is used and more than 50,000 bytes of data follows before the End expression is found, the incomplete result will be sent to the Tenable Log Correlation Engine server, and the Tenable Log Correlation Engine Splunk Client will continue with the next log.
- After an event is captured, if it contains carriage returns or line feeds, they will be converted to spaces.



Tenable NetFlow Monitor

The documentation for the most recent version of the Tenable NetFlow Monitor is currently available starting on page 38 of the following document: http://static.tenable.com/prod_docs/LCE_4.2_clients.pdf



Tenable Network Monitor

The documentation for the most recent version of the Tenable Network Monitor is currently available starting on page 41 of the following document: http://static.tenable.com/prod_docs/LCE_4.2_clients.pdf



Tenable RDEP Monitor

The documentation for the most recent version of the Tenable RDEP Monitor is currently available starting on page 46 of the following document: http://static.tenable.com/prod_docs/LCE_4.2_clients.pdf



Tenable SDEE Monitor

The documentation for the most recent version of the Tenable SDEE Monitor is currently available starting on page 49 of the following document: http://static.tenable.com/prod_docs/LCE_4.2_clients.pdf#page=49



Get Started with the Log Correlation Engine Web Query Client

The Log Correlation Engine Web Query Client is used to request event data from RESTful web services. The logs returned from queries are stored and normalized in Log Correlation Engine. Finally, the information may be searched in Tenable Security Center and can be reviewed. The process to setup and configure the Log Correlation Engine Web Query Client begins with the configuration of the RESTful API instances that are to be queried.

The Log Correlation Engine Web Query Client supports:

- [Amazon Web Services \(AWS\)](#)
- [Salesforce](#)
- [Google Cloud Platform \(GCP\)](#)



Hardware Requirements

Hardware	Minimum Requirement
Processor	Dual Core x86-64
Processor Speed	2 Ghz
Ram	2 GB
Disk Space	100 MB



Software Requirements

Operating System

The Tenable Log Correlation Engine Web Query Client is compatible with the following operating systems:

- Red Hat Enterprise Linux 6 64-bit
- CentOS 6 64-bit

Tenable Network Security

The Tenable Log Correlation Engine Web Query Client requires the following software:

- Tenable Security Center 5.1.x or later

Amazon Web Services (AWS)

To monitor AWS, an IAM user account with read-only access to CloudTrail is required.

Salesforce

To monitor Salesforce, a connected app with read permission for the LoginHistory and User objects is required.

Google Cloud Platform (GCP)

To monitor GCP, a user must be created, the Cloud Pub/Sub service must be enabled, and Stackdriver Logging must be configured.



Licensing

Tenable Security Center must be licensed for the Tenable Log Correlation Engine Web Query Client. For more information, see [Licenses](#) in the *Tenable Security Center User Guide*.



Install, Configure, and Remove

This section includes the following instructions for installing, configuring, and removing the Log Correlation Engine Web Query Client. With the exception of downloading the Web Query Client, the following procedures must be performed on the command line.

- [Download the Tenable Log Correlation Engine Web Query Client](#)
- [Install the Log Correlation Engine Web Query Client](#)
- [Configure the Log Correlation Engine Web Query Client](#)
- [Remove the Log Correlation Engine Web Query Client](#)



Install the Log Correlation Engine Web Query Client

Before you begin:

- Download the Log Correlation Engine Web Query Client, as described in [Download an Log Correlation Engine Client](#).

To install the Web Query Client:

Note: All shell commands need to be executed by a user with root privileges.

1. Copy the downloaded client package to the host where it will be installed.
2. Verify the MD5 checksum of the client package against the MD5 checksum found in the [release notes](#).

Example:

```
# md5sum lce_webquery-4.6.0-el6.x86_64.rpm
da9f07886a693fb69cba1dbd5c3eba31 lce_webquery-4.6.0-el6.x86_64.rpm
```

3. To initiate the installation, type the following command:

rpm -ivh <package name>, where **<package name>** is the name of the client package.

Example:

```
# rpm -ivh lce_webquery-4.6.0-el6.x86_64.rpm
Preparing...                               ##### [100%]
 1:lce_webquery                           ##### [100%]
Wrote UUID to /opt/tenable/tag
Please run /opt/lce_webquery/set-server-ip.sh to configure your Tenable Log
Correlation Engine server's IP and port.
```




Configure the Log Correlation Engine Web Query Client

Note: All shell commands need to be executed by a user with root privileges.

To configure the Web Query Client, you can execute the **set-server-ip.sh** script and include the Log Correlation Engine Server IP address and port number as arguments, or execute the script and, when prompted, enter the IP address and port number individually.

To execute the script using arguments:

1. Type **/opt/lce_webquery/set-server-ip.sh <IP> <Port>**, where <IP> is the IP address of an Log Correlation Engine Server and <Port> is the port number assigned to the server. By default, the port number is *31300*.

The Log Correlation Engine Server IP address and port number are updated, and the Tenable Log Correlation Engine Web Query Client daemon is restarted.

Example:

```
# /opt/lce_webquery/set-server-ip.sh 192.168.22.11 31300
Updating LCE Server IP from 192.0.2.66 to 192.0.2...
Updating LCE Server Port from 31300 to 31300...
Done
Stopping LCE Webquery daemon           [ OK ]
Starting LCE Webquery daemon           [ OK ]
```

To execute the script without arguments:

1. Type **/opt/lce_webquery/set-server-ip.sh**

You are prompted to enter the Log Correlation Engine Server IP address or hostname.

2. Type the IP address or hostname of Log Correlation Engine LCE server.

You are prompted to enter the Log Correlation Engine server port.

3. Type the port number assigned to the server for Log Correlation Engine client communication. By default, the port number is *31300*.

The Log Correlation Engine Server IP address and port number are updated, and the Log Correlation Engine Web Query Client daemon is restarted.



Example:

```
# /opt/lce_webquery/set-server-ip.sh
```

```
Enter the new desired LCE server IP or hostname.
```

```
>>
```

```
192.168.22.11
```

```
Enter the new desired LCE server port [31300].
```

```
>>
```

```
31300
```

```
Updating LCE Server IP from 203.0.113.1 to 192.168.22.11...
```

```
Updating LCE Server Port from 31300 to 31300...
```

```
Done
```

```
Stopping LCE Webquery daemon
```

```
[ OK ]
```

```
Starting LCE Webquery daemon
```

```
[ OK ]
```



Remove the Log Correlation Engine Web Query Client

Note: All shell commands need to be executed by a user with root privileges.

To remove the Log Correlation Engine Web Query Client:

1. To query the rpm database to obtain the name of the currently installed package, type **rpm -qa |grep lce_**.

Example:

```
# rpm -qa |grep lce_  
lce_webquery-4.6.0-el6.x86_64
```

2. Type **rpm -e lce_webquery**.

The Web Query Client package is removed.

Example:

```
# rpm -e lce_webquery  
warning: /opt/lce_webquery/state.json saved as /opt/lce_  
webquery/state.json.rpmsave  
warning: /opt/lce_webquery/server_assignment.xml saved as /opt/lce_  
webquery/server_assignment.xml.rpmsave
```

3. Optionally, type **rm -rf /opt/lce_webquery/** to remove the Web Query Client install directory. Configuration and log files will remain unless the directory is removed.

An additional directory, **/opt/tenable**, will be installed with the Web Query Client if it does not already exist. This directory contains a UUID that tracks all events related to the endpoint on which the client is installed. This directory should *only* be removed if no other Tenable products are in use, and no others will be installed on the endpoint in the future.



Features

This section describes the features available in the Tenable Log Correlation Engine Web Query.

- [Monitor Amazon Web Services \(AWS\)](#)
- [Monitor Salesforce](#)
- [Monitor Google Cloud Platform \(GCP\)](#)
- [Monitor and Limit Bandwidth](#)
- [Monitor Client Statistics](#)



Monitor Amazon Web Services (AWS)

The Tenable Log Correlation Engine Web Query Client queries the AWS CloudTrail API in order to [monitor events supported by CloudTrail](#). These events can be viewed in Tenable Security Center and used to identify irregular activity in AWS. In order to [monitor CloudTrail events](#), you must enable CloudTrail, attach the necessary policy to IAM users or groups, and configure the Web Query Client policy to make calls to the CloudTrail API. Additionally, you can [limit the amount of bandwidth the Web Query Client will use](#) when communicating with CloudTrail, and [monitor the hardware statistics](#) of the host where the Web Query Client is installed.



Monitor Salesforce

The Tenable Log Correlation Engine Web Query Client queries the Salesforce REST API in order to monitor login events, as well as the creation and modification of user accounts. These events can be viewed in Tenable Security Center and used to identify irregular activity in Salesforce from unexpected sources. In order to [monitor Salesforce events](#), you must create a connected app, and configure the Web Query Client policy to make calls to the Salesforce API. Additionally, you can [limit the number of calls the Web Query Client will make](#) to the Salesforce API to respect subscription limits, and [monitor the hardware statistics](#) of the host where the Web Query Client is installed.



Monitor Google Cloud Platform (GCP)

The Tenable Log Correlation Engine Web Query Client queries the Google Cloud API and the Google Cloud Pub/Sub service in order to monitor various events that you can specify when configuring logging in GCP. In order to [monitor GCP events](#), you must enable the Pub/Sub API in Google Cloud, set up a topic, and configure the Web Query Client policy to make calls to the Pub/Sub service. Additionally, you can [limit the number of calls the Web Query Client will make](#) to the Pub/Sub service, and [monitor the hardware statistics](#) of the host where the Web Query Client is installed.



Monitor and Limit Bandwidth

The Tenable Log Correlation Engine Web Query Client monitors the number of calls made and bandwidth used while communicating with the Salesforce and AWS CloudTrail APIs. The monitored data can be viewed in Tenable Security Center. Additionally, when you configure a Web Query Client policy, you may specify limits on the number of calls or the amount of bandwidth the Web Query Client will use over a period of time. This feature can be leveraged to reduce costs related to AWS, or respect the call limit imposed by a Salesforce subscription, among other potential uses. Warnings are generated when usage reaches thresholds of 50%, 75%, and 90% of the defined limit.



Monitor Client Statistics

All Tenable Log Correlation Engine clients monitor the hardware statistics of the host where the client is installed. The hardware statistics can be viewed via the Tenable Log Correlation Engine server interface and Tenable Security Center. These statistics can be used to evaluate the resource and network usage of the host while the Tenable Log Correlation Engine client is operating.



How To

This section describes how to perform the actions available in Tenable Log Correlation Engine Web Query Client.

You can configure the Web Query Client to query [AWS CloudTrail](#), [Salesforce](#), and [Google Cloud Platform](#) in order to track and review events.



How to Monitor Amazon Web Services (AWS)

This section describes the steps necessary to query AWS with the Tenable Log Correlation Engine Web Query Client.

1. [Complete the prerequisite tasks in AWS.](#)
2. [Configure the Web Query Client policy.](#)
3. [Review AWS events in Tenable Security Center CV.](#)



Prerequisite Tasks for Integration with AWS

Before querying AWS with the Tenable Log Correlation Engine Web Query Client, you must perform the following tasks in AWS:

1. [In the AWS console, enable CloudTrail.](#)
2. [Create one or more IAM users.](#)
 - Generate an access key for each user.
 - Download the user security credentials.
3. [Attach the AWSCloudTrailReadOnlyAccess policy to each user, or the group that contains the users, created in step 2.](#)
4. [Configure a Web Query Client policy to query CloudTrail.](#)



Configure the Web Query Client Policy for AWS

Using the [Client Policy Builder](#), you can create and modify policies for your Tenable Log Correlation Engine Web Query Client. The following steps are performed via the web interface on the Tenable Log Correlation Engine server that you configured your Tenable Log Correlation Engine Web Query Client to communicate with.



To configure the Web Query Client Policy for AWS:

1. Using the Client Policy Builder, [create a policy for your Tenable Log Correlation Engine Web Query Client](#). This documentation includes a list of [valid configuration items for the client policy](#).

A Web Query Client policy for AWS requires you to add an AWS CloudTrail endpoint to the policy. You must provide the following:

- The User ID and secret key [that was created when completing the prerequisite tasks](#).

To add the endpoint:

- a. In the **Basic** pane of the Client Policy Builder, click the  button in  to add a group.

The **Add a new endpoint group** window appears.

- b. Click the **Add AWS CloudTrail endpoint** button.

A new AWS CloudTrail endpoint appears.

- c. In the **Endpoint name** box, enter a name that identifies the endpoint.
- d. Select the **Active** check box.
- e. In the **Query interval** box, enter the number of seconds between each query to the Salesforce API.
- f. In the **Region** box, enter the region defined in the AWS account.
- g. In the **Access Key ID** box, enter the Access Key ID for an IAM user.
- h. In the **Secret Access Key** box, enter the IAM Secret Access Key that corresponds to the Access Key ID.



Note: You can add multiple endpoints to a single group. For example, one group could contain three AWS CloudTrail endpoints. Another group could contain a Salesforce endpoint, an AWS CloudTrail endpoint, and a Google Cloud endpoint.

2. [Assign the policy to the Tenable Log Correlation Engine Web Query Client.](#)



Review AWS Events in Tenable Security Center

To review AWS Events in Tenable Security Center:

1. Navigate to Tenable Security Center and log on with a user account that has permission to view logs for the organization.

A dashboard that corresponds to the user role appears.

2. In the top navigation bar, click **Analysis**, and then click the **Events** link.

The **Event Analysis** page appears, displaying the **Type Summary** section.

3. Click the **Type Summary** button, and then select **Normalized Event Summary**.

The **Normalized Event Summary** section appears.

4. In the upper-left corner of the page, click **>>**.

The **Filters** pane appears.

5. Click the **Select Filters** button

6. In the **Add Filter** window, select **Normalized Event**.

7. Click the **Apply** button.

8. Click the **Normalized Event** box.

9. In the **Normalized Event** window, type **AWS-***.

10. Click **OK**.

11. In the **Filters** pane, click the **Apply All** button.

In the **Normalized Event Summary** section, the list of events is filtered and displays only events that start with **AWS-**.

The AWS events available will be based on the monitored activity logged by AWS CloudTrail. For a list of specific events, you can click an AWS event type (e. g., **AWS-Console_Login**) listed in the **Normalized Event Summary** section. You can also click the **Jump to Raw Syslog Events** link to directly view the log data.



12. At the top of the **Event Analysis** page, click the **Normalized Event Summary** button, and then select **Detailed Event Summary**.

The **Detailed Event Summary** section appears.

For a list of specific events, click an AWS event (e. g., ConsoleLogin) listed in the **Detailed Event Summary** section.



How to Monitor Salesforce

This section describes the steps necessary to query Salesforce with the Tenable Log Correlation Engine Web Query Client.

1. [Complete the prerequisite tasks in Salesforce.](#)
2. [Configure the Web Query Client policy.](#)
3. [Review Salesforce events in Tenable Security Center.](#)



Prerequisite Tasks for Integration with Salesforce

Before completing the procedures to integrate Tenable Log Correlation Engine with Salesforce, you must perform the following tasks in Salesforce:

1. [Create a connected app.](#)
 - Give the app read permission for the LoginHistory and User objects.
 - Save the Consumer Secret and Consumer Key.

2. [Relax IP restrictions.](#)

Note: This task is only necessary if you are unable to view Salesforce events in Tenable Security Center.

3. [Configure a Web Query Client policy to query the Salesforce REST API.](#)



Configure the Web Query Client Policy for Salesforce

Using the [Client Policy Builder](#), you can create and modify policies for your Tenable Log Correlation Engine Web Query Client. The following steps are performed via the web interface on the Tenable Log Correlation Engine server that you configured your Tenable Log Correlation Engine Web Query Client to communicate with.



To configure the Web Query Client Policy for Salesforce:

1. Using the Client Policy Builder, [create a policy for your Tenable Log Correlation Engine Web Query Client](#). This documentation includes a list of [valid configuration items for the client policy](#).

A Web Query Client policy for Salesforce requires you to add a Salesforce endpoint to the policy. You must provide the following:

- The username, password, and security token of a Salesforce user account.
- The Consumer Secret and Consumer Key [you obtained when you created a connected app](#).

To add the endpoint:

- a. In the **Basic** pane of the Client Policy Builder, click the  button in  to add a group.

The **Add a new endpoint group** window appears.

- b. Click the **Add Salesforce endpoint** button.

A new Salesforce endpoint appears.

- c. In the **Endpoint name** box, enter a name that identifies the endpoint.
- d. Select the **Active** check box.
- e. In the **Query interval** box, enter the number of seconds between each query to the Salesforce API.
- f. In the **Username** box, enter the username for the Salesforce account being queried.



- g. In the **Password** box, enter the password that corresponds to the username, along with that user's security token appended to the end of the password. For example, passwordsREvNGuKHvuIhLTrS.
- h. In the **Consumer Key** box, enter the Consumer Key for the connected app you created.
- i. In the **Consumer Secret** box, enter the Consumer Secret for the connected app you created.

Note: You can add multiple endpoints to a single group. For example, one group could contain three Salesforce endpoints. Another group could contain a Salesforce endpoint, an AWS CloudTrail endpoint, and a Google Cloud endpoint.

2. [Assign the policy to the Tenable Log Correlation Engine Web Query Client.](#)



Review Salesforce Events in Tenable Security Center

To review Salesforce Events in Tenable Security Center:

1. Navigate to Tenable Security Center and log on with a user account that has permission to view logs for the organization.

A dashboard that corresponds to the user role appears.

2. In the top navigation bar, click **Analysis**, and then click the **Events** link.

The **Event Analysis** page appears, displaying the **Type Summary** section.

3. Click the **Type Summary** button, and then select **Normalized Event Summary**.

The **Normalized Event Summary** section appears.

4. In the upper-left corner of the page, click [»](#).

The **Filters** pane appears.

5. Click the **Select Filters** button, and then, in the **Add Filter** popout, select **Normalized Event**.

6. Click the **Apply** button.

7. Click the **Normalized Event** box, and then, in the **Normalized Event** text box, type *Salesforce-**.

8. Click **OK**.

9. In the **Filters** pane, click the **Apply All** button.

In the **Normalized Event Summary** section, the list of events is filtered and displays only events that start with *Salesforce-*.

For Salesforce, the Web Query Client monitors login successes and failures, and the creation and modification of user accounts. For a list of specific events, click a Salesforce event type (e. g., *Salesforce-Remote_Access_Login*) listed in the **Normalized Event Summary** section. You can also click the **Jump to Raw Syslog Events** link to directly view the log data.



How to Monitor GCP

This section describes the steps necessary to query GCP with the Tenable Log Correlation Engine Web Query Client.

1. [Complete the prerequisite tasks in GCP.](#)
2. [Configure the Web Query Client policy.](#)
3. [Review GCP events in Tenable Security Center CV.](#)



Prerequisite Tasks for Integration with GCP

Before completing the procedures to integrate Tenable Log Correlation Engine with GCP, you must perform the following tasks via the [GCP Console](#):

1. [Create a service account for Tenable Log Correlation Engine](#). When you create the service account:
 - Select **Furnish a new private key**.
 - For **Key type**, select **JSON**.

A .json file that contains the public/private key pair is downloaded. This key pair is required for the Web Query Client policy.

Note: The previous link is to the official documentation for GCP. This procedure expects that you will be using the GCP Console to complete the tasks. After viewing the official GCP documentation, to see the instructions for the Console, in the boxes that appear on the page, click **Console**.

For example:

REST **CONSOLE** GCLOUD

- Open the **Service Accounts** page in the Cloud Platform Console.

OPEN THE SERVICE ACCOUNTS PAGE

- Click **Select a project**.
- Select your project and click **Open**.
- Click **Create Service Account**.
- Enter a service account name, select a role you wish to grant to the service account and click **Create**.

2. If you have not already, [complete the steps required to enable the Pub/Sub API](#). Then, [create a topic and add a subscription](#).
 - For **Delivery Type**, select **Pull**.

Note the subscription name. The subscription name is required for the Web Query Client policy.



Note: The previous links are to the official documentation for the Pub/Sub service. It includes sections about publishing a message to a topic, pulling the message from a subscription, and cleaning up. For the purpose of this procedure, those sections can be ignored.

3. If you want to you want to obtain logs from one or more Google Compute Engine or Amazon EC2 VM instances, [install the logging agent on those instances](#).
4. [Configure Stackdriver Logging to export one or more logs](#) to the topic you created in step 2. Those logs will be processed by the Web Query Client.
5. [Configure a Web Query Client policy to pull logs from the Pub/Sub service](#).



Configure the Web Query Client Policy for GCP

Using the [Client Policy Builder](#), you can create and modify policies for your Tenable Log Correlation Engine Web Query Client. The following steps are performed via the web interface on the Tenable Log Correlation Engine server that you configured your Tenable Log Correlation Engine Web Query Client to communicate with.



To configure the Web Query Client Policy for GCP:

1. Using the Client Policy Builder, [create a policy for your Tenable Log Correlation Engine Web Query Client](#). This documentation includes a list of [valid configuration items for the client policy](#).

A Web Query Client policy for GCP (Google Cloud Platform) requires you to add a Google Cloud endpoint to the policy. You must provide the following:

- The service account key in the .json file that was [downloaded when completing the prerequisite tasks](#).
- The subscription name for the Pub/Sub service topic.

To add the endpoint:

- a. In the **Basic** pane of the Client Policy Builder, click the  button in  to add a group.

The **Add a new endpoint group** window appears.

- b. Click the **Add Google Cloud endpoint** button.

A new Google Cloud endpoint appears.

- c. In the **Endpoint name** box, enter a name that identifies the endpoint.
- d. Select the **Active** check box.
- e. In the **Query interval** box, enter the number of seconds between each query to the Cloud Pub/Sub service.
- f. In the **JSON service account key** box, enter the entire service account key including the braces.



For example:

```
{
  "type": "service_account",
  "project_id": "blinkum-genovese-011599",
  "private_key_id": "d644c15c7332d29574f0f36ec31659db2e7cdad2",
  "private_key": "-----BEGIN PRIVATE KEY-----
\nPmxlQ6i3kz/s07NtLX2lcRuUAzgHiET99UALqLWGsF2Msqfb38rtvBfF0mTg+NOQH8BkX8Xbh-
GPN1Ks4xDHxtgKbSvWlUg+Eit3rSp1NuWjSz7YqUuCSgsOwbbRQvXtNKvr2R1lbFyyymMpakB6i-
XT5UnfJqftZa5M6pWlMt2wikmkRQxlpJTHPmaRr3fyhnYJqM/v\TJL4bjprvuYSqzMixaWq0\F-
o0ND28kB30dAhhao5NM6oykq8\OdYc6v534Y+eQfcpkOCN8qRyTTzyYLh0fKm2vEz0/O2n7+jm3-
1h/zNlLqXf/87HsKE8TwGqw05xi121XlrL3\j8DKrNuYy9UClaxxND/r8ncgK6Cv\AYp1DJ1qLw-
2aIndYZa9iXyvVQ5GdpUazj0eH0RbibfjMCwP1di0Alnm1XfYmK3hTjT2/+teZtOp1DL/40Czu-
P\k3foR5\G5aTFKo2+w8N5wmtg5ehvDsmMmvfP2TPxIZia6BPD0uyKdESMOZ0fsEgSNSFPoaIUq-
/qV1IrA7Q2XwtGzWuqDcALJi7x65IxrIivXUrHv379AjgrXW6SnKEFLJ1LtHi9dGBElNI+h3mx+-
\\z\v0X8d1vJed4tjOMNvWRaAhXhuNouAly7Xt3Eug9OCTX+di9esV7kF++heG/8yQLIQCyEBRM-
fot4SnDvw7xJ0sKSOKv5MOi8t6HGLsggvFR5R6V6l3BwqeljYJDND0YInFYKcI3DUQ8aumNLOJ-
fEi2st9pR2sH6xb7sKSF5odeSk0oAEPqDBoOrTrYdjMUX/uRTfZBRkhKH3zVGqWR8E4HWLYnuy5-
vr/yEiJ/xjTS1SfVQ+mw2vVq3UdrGhP0yJelJvGAi6FAccIaJV4LkGrEKjYA6v06n2Gswt4pR\F-
Z6IQj9CU8D5rUnmuJ9VP302ivHWkXWIBZzUZjFI3TWRZWncZXhQ8ySki6cHW7ng06WsQeN2wFP0-
UHHPCqkeQo1VOL+5e3P0gb0izNCdy3a+ffk9XrMZo91MvyqdwPL0unI6cgcoTL1slDgwrbyvcjU-
AcYG6iI6/CC5o5ws\5CN1I1/JgE1IQ1I48815H+q/67GUaywyR2Sfd\c4nRcNRUMJNWjzzntjra-
AhBy19NmKaEWKitgSFQIf1o9uatXo4s\0cPzL2ejY2bTF+1Sgo1yatsg5UWZjhb0dPabiAWKQJJo-
Zmilq7jKJ++o\ayooY0VR1kimXuhix9Rr1KLsRy0vL4KjnY3Rg2UTI5zoPyAdr4VFTsLuZ8\0WM-
F8/BxcASBhPCu9f4YI9hL3Qnhf4sV2+cMDUR71uv7LXIzhsaz9TDDKRvqyEoRGVo1EiNjC1CrF4-
IPzDRwfRoAD7SegAKt5gLF+XkE5PwrVqYD9iTxj7tK\yyOR9nRRswgsz3MW78hVJXKcvSVh06m\
-2S55MiSBp/Qm4U9Rjtnpy1SwNc8818A6DKQtUFM/R+rR\Nl9pmMo2yPBNRX+5F0KMKRsvYuDWuh-
gvXmWIV19I8+Aif4kh9XUpJBQtrHrFD1wRDQ2HNV+vgklewhMOiHmSqTc5oZlNQmOH0+dgKwkkN-
gc12yu/z5FS0xm\bl0b+fZ54KI3lJa45jJyq3+BMyN0pJ\nIWoSRqSIbyD/TlmGsfgzoQLTrUm1-
SgLh2RkmaCogdBlsGg6hD2C8Uf\n-----END PRIVATE KEY-----\n",
  "client_email": "test-credential-service-acct@blinkum-genovese-
011599.iam.gserviceaccount.com",
  "client_id": "404842616201342653591",
  "auth_uri": "https://accounts.google.com/o/oauth2/auth",
  "token_uri": "https://accounts.google.com/o/oauth2/token",
  "auth_provider_x509_cert_url":
  "https://www.googleapis.com/oauth2/v1/certs",
```



```
"client_x509_cert_url":  
"https://www.googleapis.com/robot/v1/metadata/x509/test-credential-service-  
acct%40blinkum-genovese-011599.iam.gserviceaccount.com"  
}
```

- g. In the **Subscription** box, enter the subscription name. For example, projects/my-project-name/subscriptions/my-subscription-name.

Note: You can add multiple endpoints to a single group. For example, one group could contain three Google Cloud endpoints. Another group could contain a Salesforce endpoint, an AWS CloudTrail endpoint, and a Google Cloud endpoint.

2. [Assign the policy to the Tenable Log Correlation Engine Web Query Client.](#)



Review GCP Events in Tenable Security Center

To review GCP Events in Tenable Security Center:

1. Navigate to Tenable Security Center and log on with a user account that has permission to view logs for the organization.

A dashboard that corresponds to the user role appears.

2. In the top navigation bar, click **Analysis**, and then click the **Events** link.

The **Event Analysis** page appears, displaying the **Type Summary** section.

3. Click the **Type Summary** button, and then select **Normalized Event Summary**.

The **Normalized Event Summary** section appears.

4. In the upper-left corner of the page, click [»](#).

The **Filters** pane appears.

5. Click the **Syslog Text** box, and then, in the **Syslog Text** text box, type *googleapis*.

6. Click **OK**.

7. In the **Filters** pane, click the **Apply All** button.

In the **Normalized Event Summary** section, the list of events is filtered and displays events that include *googleapis* in the text of the syslog.

The GCP events available will be based on the logs you specified [when you configured Stackdriver Logging](#). You can click the **Jump to Raw Syslog Events** link to directly view the log data.



Additional Resources

This section contains the following additional resources:

- [Web Query Client Policy Configuration Items](#)
- [Correcting AWS Configuration Issues](#)
- [Correcting Network Time Protocol Issues](#)



Web Query Client Policy Configuration Items

The interaction of the Web Query Client with AWS, Salesforce, and GCP is configured by modifying a Web Query Client policy via the Client Policy Builder. The policy is separated into configurable items, represented in the **Advanced** pane of the Client Policy Builder by XML elements of the same name. Certain parameters are common to all Tenable Log Correlation Engine clients and are generally the parameters listed first in a policy.

The usage and application parameters that follow the common client parameters vary based on the client. In the case of the Web Query Client policy, parameters are provided that allow you to limit the bandwidth the Web Query Client will use, as well as specify the credentials required for connecting to AWS, Salesforce, and GCP.

This section includes:

- [Example: **default_rhel_web** Policy](#)
- [Common Client Parameters](#)
- [Usage-Limit Parameters](#)
- [CloudTrail Parameters](#)
- [Salesforce Parameters](#)
- [GCP Parameters](#)

Example: **default_rhel_web** Policy

The following is an example of the contents of a Web Query Client policy file.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<options xmlns:xi="http://www.w3.org/2003/XInclude">
  <log-directory>/opt/lce_webquery/logs</log-directory>
  <debug-level>INFO</debug-level>

  <!--<local-ip-net>192.0.2.0/24</local-ip-net>-->

  <!-- client-debug / -->
  <heartbeat-period>300</heartbeat-period>
  <statistics-period>60</statistics-period>
```



```
<compress-events>1</compress-events>
<group>
</group>

<!-- Group Setup Example
<group>
  <name>ByteRestrictedGroup</name>
  <usage-limit>
    <type>BYTES</type>
    <value>35M</value>
    <time>MONTH</time>
    <start-day>5</start-day>
  </usage-limit>
  <cloudtrail>
    <name>CloudTrail1</name>
    <active>yes</active>
    <query-interval-seconds>600</query-interval-seconds>
    <region>us-east-1</region>
    <id>AWSId</id>
    <key>MySecretKey</key>
  </cloudtrail>
</group>
<group>
  <name>CallRestrictedGroup</name>
  <usage-limit>
    <type>CALLS</type>
    <value>10000</value>
    <time>DAY</time>
  </usage-limit>
  <salesforce>
    <name>Salesforce_1</name>
    <active>no</active>
    <query-interval-seconds>300</query-interval-seconds>
    <username>MyUsername</username>
    <password>MyPassword</password>
    <consumer-key>MyKey</consumer-key>
    <consumer-secret>MySecret</consumer-secret>
  </salesforce>
</salesforce>
```



```
<name>Salesforce_2</name>
<active>yes</active>
<query-interval-seconds>450</query-interval-seconds>
<username>MyUsername</username>
<password>MyPassword</password>
<consumer-key>MyKey</consumer-key>
<consumer-secret>MySecret</consumer-secret>
</salesforce>
</group>
-->
</options>
```

Common Configuration Items

The following table lists the policy configuration items in the order they appear in the default Web Query Client policy. These parameters are defined when configuring the Web Query Client policy for AWS, Salesforce, and [GCP](#).

Configuration Item	Description	Example
log-directory	The path to which to write the Web Query Client operational logs.	/opt/lce_webquery/logs
debug-level	Minimum debugging level that is printed to the log. The options supported are as follows: <ul style="list-style-type: none">• INFO• WARN• ERROR• NONE	INFO
local-ip-net	If a host has multiple network connections, allows you to specify which network to use. If not set or if the CIDR does not match any networks, the client will use the first network connection detected.	192.0.2.0/24



Configuration Item	Description	Example
heartbeat-frequency	The number of seconds between each client heartbeat message to the Tenable Log Correlation Engine server. If set to 0, the client will not send heartbeats.	A positive integer. 300
statistics-frequency	The number of minutes between each client host performance statistics report (CPU, Disk Space, and Physical Memory) to the Tenable Log Correlation Engine server. If set to 0, client statistics will not be sent.	A positive integer. 60
compress-events	Defines whether to compress events before transmitting them to the Tenable Log Correlation Engine server. If set to 1, provides a marginal savings for bandwidth in exchange for a marginal increase in CPU usage.	0 (off) or 1 (on)
Write events to standard output	Whether to write events to standard output (stdout). Any event picked up by the Tenable Log Correlation Engine Splunk Client will have the raw log printed to the stdout of the client, the default being a terminal session, before the client sends it to the Tenable Log Correlation Engine server to be processed. This configuration item is useful for debugging and troubleshooting.	0 (off) or 1 (on)

Usage-Limit Configuration Items

The configuration of the usage-limit items is usually based on the API being queried. The AWS CloudTrail API measures the amount of bandwidth utilized by the queries made to the API. The Salesforce API measures the number of calls. Because CloudTrail and Salesforce monitor usage differently, generally groups will be limited by bytes or calls based on the API. However, the Web Query Client can be configured to support many use cases, such as limiting usage of the Salesforce API by bytes. The usage limit parameters are in place to help control excess bandwidth charges, and



respect call limitations that are applied by the API vendor.

The following table lists the usage-limit parameters in the order they appear in the Client Policy Builder. These parameters are defined when configuring a Web Query Client policy for [AWS](#), [Salesforce](#), or [GCP](#).

Configuration Item	Description	Example Value
name	An alphanumeric name for the connection group.	ByteRestrictedGroup
type	Groups can either be limited by BYTES or CALLS	BYTES
value	<div>This is the numeric value given to BYTES or CALLS. Note: Bytes can be represented by a number followed by K(Kilobyte), M(Megabyte) G (Gigabyte), or T(Terabyte).</div>	100M
time	The period of time by which usage is limited. For example, if a group is limited to 1000 calls, and this parameter is set to DAY, usage is limited to 1000 calls every 24 hours.	MONTH, DAY, HOUR, MINUTE
start-day	Defines the starting day when the <i>time</i> parameter is set to <i>MONTH</i> . The value can be an integer from 1 to 28.	14

CloudTrail Parameters

The following table lists the CloudTrail parameters in the order they appear in the Client Policy Builder. These parameters are defined when configuring a Web Query Client policy for [AWS](#).



Policy Parameter	Description	Example Value
name	An alphanumeric name for the CloudTrail connection.	AWSgroup
active	Defines whether to query the instance. If set to yes, the Web Query Client will make queries using the parameters defined in that CloudTrail subsection. You can have multiple subsections that are configured to be active.	yes
query-interval-seconds	The number of seconds between each query to the endpoint.	300
region	The region defined in the AWS account.	us-east-1
id	An IAM Access Key ID.	IKADY6VH42HTKTQI4OA
key	The IAM Secret Access Key that corresponds to the Access Key ID.	koN/ByNBZB5S7/tOrT3WBrGD9dQjDvT98bU9qpyH



Salesforce Parameters

The following table lists the Salesforce parameters in the order they appear in the Client Policy Builder. These parameters are defined when configuring a Web Query Client policy for [Salesforce](#).

Policy Parameter	Description	Example Value
name	An alphanumeric name for the Salesforce connection.	SalesforceGroup
active	Defines whether to query the instance. If set to yes, the Web Query Client will make queries using the parameters defined in that Salesforce subsection. You can have one or more subsections in multiple groups that are configured to be active.	yes
query-interval-seconds	The number of seconds between each query to the	300



Policy Parameter	Description	Example Value
	endpoint.	
username	The username for the Salesforce account being queried.	user@example.com
password	The password that corresponds to the username, and that user's security token appended to the end of the password.	passwordsREvNGuKHvulhLTrS
consumer-key	The Consumer Key for a connected app.	1MVG7KI2HHAq08RzmvrJMfFaXELNe_ Tbg1vJf.xUyRK7f5Hyso2bZrW.TobC9XQ.jqzNVP0ytuD_ 1XrKKFsku
consumer-secret	The Consumer Secret for a connected app.	8675309731701479235

GCP Parameters

The following table lists the GCP parameters in the order they appear in the Client Policy Builder. These parameters are defined when configuring a Web Query Client policy for [GCP](#).

Policy Parameter	Description	Example Value
name	An alphanumeric name for the	GCP



Policy Parameter	Description	Example Value
	GCP group.	
active	Defines whether to query the instance. If set to yes, the Web Query Client will make queries using the parameters defined in that GCP subsection. You can have one or more subsections in multiple groups that are configured to be active.	yes
query-interval-seconds	The number of seconds between each query to the endpoint.	300
json-service-account-key	The service account key for a GCP user.	The contents of a .json file downloaded from GCP.
Subscription	The subscription name for the Google Pub/Sub service topic.	projects/example-project080116/subscriptions/logging-feed-topic



Correcting AWS Configuration Issues

The AWS command line interface (CLI) can be installed to troubleshoot AWS connection and configuration issues. Information about installation of AWS CLI can be found [here](#).

To correct AWS configuration issues:

1. The first command will configure the AWS CLI. If it was previously ran the AWS Access Key ID, AWS Secret Access Key, and region name will already be populated. This information is also found in the policy file. An example of the output from this command is shown below.

```
C:\>aws configure
AWSAccess Key ID [*****JSQJ]:
AWS SecretAccess Key [*****yaGQ]:
Default region name [us-west-2]:
Default output format [None]:
```

2. The second command will describe trails that are available if the configuration criterion was entered correctly in the previous step. It will also provide the names of the trails that are available to be queried. An example of the output from this command is shown below.

```
C:\>aws cloudtrail describe-trails
{
  "trailList": [
    {
      "IncludeGlobalServiceEvents": true,
      "Name": "test_trail",
      "TrailARN": "arn:aws:cloudtrail:us-west-2:920172477660:trail/test_trail",
      "LogFileValidationEnabled": false,
      "S3BucketName": "client-api-test-bucket",
      "CloudWatchLogsRoleArn": "arn:aws:iam::920172477660:role/CloudTrail_CloudWatchLogs_Role",
      "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-west-2:920172477660:log-group:CloudTrail/DefaultLogGroup:*"
    }
  ]
}
```



3. Using the name of the trail you can query the trails status. From the output, you can tell if the trail is logging and the start and stop logging time in Epoch time of the trail. An example of the output from this command is shown below.

```
C:\>aws cloudtrail get-trail-status --name test_trail {
  "LatestNotificationAttemptSucceeded": "",
  "LatestDeliveryAttemptTime": "2015-11-02T05:04:50Z",
  "LatestDeliveryTime": 1446440690.306,
  "TimeLoggingStarted": "2015-10-26T21:43:08Z",
  "LatestDeliveryAttemptSucceeded": "2015-11-02T05:04:50Z",
  "IsLogging": true,
  "LatestCloudWatchLogsDeliveryTime": 1446243728.775,
  "StartLoggingTime": 1445895788.299,
  "StopLoggingTime": 1444418827.475,
  "LatestNotificationAttemptTime": "",
  "TimeLoggingStopped": "2015-10-09T19:27:07Z"
}
```




Correcting Network Time Protocol Issues

If you are not receiving any AWS events, and the message below is found in the logs Network Time Protocol (NTP), it should be checked to ensure it is configured correctly.

```
Oct 28, 15 14:38:26.898556 (endpoint_0) INFO (webquery_
endpoint.cpp:168,sendHealthStatus) - LCE Web Client Status: Alert: Endpoint
Demo/CloudTrail-test-Cloud: CloudTrail query signature was invalid, and no further
queries will be submitted. Check your system clock and timezone. To resume querying,
update the system clock or restart the client.
```

To correct Network Time Protocol issues:

1. Running the clock or date command will show the current time of the server.

```
# clock
Wed 04 Nov 2015 04:33:29 PM EST -0.266432 seconds
# date
Wed Nov 4 16:33:32 EST 2015
```

2. The following command can be run to re-sync the time with the configured NTP servers if the time is found to be incorrect.

```
# ntpd -qg
ntpd: time set -6.953726s
```

3. After the time is has been re-synced stop the Log Correlation Engine Web Query Client using the command below.

```
# service lce_webquery stop
```

4. Remove the state.json file from the /opt/lce/webquery directory.

```
# rm -rf /opt/lce_webquery/state.json
```



5. Start the Log Correlation Engine Web Query Client.

```
# service lce_webquery start
```



WMI Monitor Client

The documentation for the most recent version of the WMI Monitor Client is currently available starting on page 30 of the following document: http://static.tenable.com/prod_docs/LCE_4.2_clients.pdf



Additional Resources

This section includes the following:

- [Tools](#)
- [Encryption Strength](#)
- [File and Process Allow List](#)
- [Import Log Correlation Engine Data Manually](#)
- [Manual Key Exchange with Tenable Security Center](#)
- [User Tracking](#)
- [Non-Tenable License Declarations](#)
- [Silo Archiving](#)



Tools

When Tenable Log Correlation Engine is installed, it includes a number of tools and utilities. All tools are installed in the `/opt/lce/tools/` directory.

General Tools

The following table lists in alphabetical order each tool and describes its function.

Tool	Description	Usage
archival-manager	Performs tasks relating to archiveDb. For more information, see Silo Archiving .	<pre>--list-snapshots [<silosName> -<N_newest> <N_oldest>] --enum-snapshots [<silosName>] (Faster but less informative than --list-snapshots.) --archive <silosName> --restore <snapshotId> [<into_silosName>] --remove-active <silosName> --remove-archived <snapshotId> --archive--range [--dry-run] <from_date> <to_date> --restore--range [--dry-run] <from_date> <to_date> --remove-active--range [--dry-run] <from_date> <to_date> --remove-archived--range [--dry-run] <from_date> <to_date> (Each date must be given in YYYYMMDD format. A range includes both "to" and "from" dates. Dates refer to tOrigin of contained events.) --identify-curr-silo --roll-curr-silo-now</pre> <div>Note: Each date must be given in YYYYMMDD format.</div>



Tool	Description	Usage
		<div>A range includes both "to" and "from" dates. Dates refer to tOrigin of contained events.</div>
cfg-utils	Used to manipulate Tenable Log Correlation Engine Server configuration attributes that do not appear in the web UI. Tenable Support may ask you to perform administrative tasks with this utility.	<p>The most commonly used actions are:</p> <div>--help --list-all --like <case-ignored substring of K> --describe <K> --get <K> --vlike <case-ignored substring of K> --set-sv <K> <V></div> <p>To see the complete list of available actions, run:</p> <div>cfg-utils --help</div> <p>For information about configuring site policies related to user activity, see Site Policies.</p> <div>Tip: You can use <code>cfg-utils</code> to configure certificate-authenticated web UI logins. For more information, see Certificate-Authenticated Web UI Logins.</div>
change-activeDb-location	Changes the root directory of the operational Tenable Log Correlation Engine datastore from the default.	<div><absolute path of new location></div>
change-tracelogs-location	Changes the root directory of the Tenable Log Correlation Engine	<div><absolute path of new location></div>



Tool	Description	Usage
	tracelogs from the default.	
<code>create--make-current--silo</code>	If silo rolling is inoperable, this utility can be used (with all Tenable Log Correlation Engine daemons stopped) to switch to a new silo.	<code><siloNumber> --take-next</code>
<code>check_fix-file_accessibility</code>	Detects and fixes file accessibility problems like wrong ownership, wrong permissions, and inadvertently set immutable (“i”) extended file attribute. Normally, invoke with <code>--normal</code> .	<code>--check-only --normal</code>
<code>ha-manager</code>	Configures, manages, or disables high availability. For more information about high availability configurations, see High Availability .	<code>--initialize-as-master <standbyIP> <i/f> <virtualIP></code> <code>--initialize-as-standby <masterIP> <i/f> <virtualIP></code> <code>--copy-SSH-keys-to-peer</code> <code>--status</code> <code>--disconnect</code> <code>--de-configure</code> For more information, see:



Tool	Description	Usage
		<ul style="list-style-type: none">• Configure High Availability• Monitor Your High Availability Configuration• Disable High Availability
import_logs	Imports a directory of log files or a list of one or more logs on disk into the active database on the Tenable Log Correlation Engine server. You must specify whether the logs you are importing are encoded as ASCII (--ASCII) or UTF-8 (--UTF8).	<pre>--ASCII --UTF8 [--now-as-timestamp --may-guess-timestamps] [--minimum-timestamp-epoch <N>] [--maximum-timestamp-epoch <N>] [--no-eval-event-rules] <inputFileAbsolutePath></pre> <p>For more information about import_logs usage, see Import Log Correlation Engine Data Manually.</p>
install-PostgreSQL-man-pages		For the description and usage, see install-PostgreSQL-man-pages .
lce_crypto_utils	Used to generate and manipulate SSL credential files in the /opt/lce/credentials/syslog and /opt/lce/credentials/web_UI directories.	<pre>--generate-creds-cryptSyslog [<CA_dnSpec>] [<endEntity_dnSpec>] (NB: any prior contents of /opt/lce/credentials/syslog/ will be erased.) --generate-creds-vulnReporter [-q] (Will prompt for cert generation parameters, unless -q.) (NB: any prior contents of /opt/lce/reporter/ssl/ will be erased.) --generate-creds-webUI [-q]</pre>



Tool	Description	Usage
		<p>(Will prompt for cert generation parameters, unless -q.)</p> <p>(NB: any prior contents of /opt/lce/credentials/web_UI/ will be erased.)</p> <p>--is-signed-by <endEntity_cert_path>.pem <CA_cert_path>.pem</p> <p>--is-revoked-per <endEntity_cert_path>.pem <CRL_path>.pem</p> <p>--save-as-PKCS12 <endEntity_cert_path>.pem <endEntity_privkey>.pem <into_path>.pfx</p> <p>(Will prompt for password, and again to confirm.)</p> <p>--print-cert <endEntity_cert_path>.pem</p> <p>--print-CRL <CRL_path>.pem</p> <p>--print-privkey <privkey_path>.pem</p> <p>--print-PKCS12 <PKCS12_path>.pfx</p> <p>(Will prompt for password.)</p> <p>--what-is <path></p> <hr/> <p>A <dnSpec> is a , -separated list of K=V pairs, all optional save the last; \-escape as needed:</p> <p>'C=<country>,ST=<state>,L=<city>,O=<org>,OU=<orgUnit>,CN=<name>'</p> <div>Tip: To rotate your web UI credentials using lce_crypto_utils, see Rotate Web UI Credentials.</div>
list-clients	Used to list clients since Log Correlation Engine 5.0.3.	<p># /opt/lce/tools/list-clients</p> <div>Note: The --brief option can be used for brief output. The default output is verbose.</div>



Tool	Description	Usage
list-policies	Used to list policies since Log Correlation Engine 5.0.4.	<pre># /opt/lce/tools/list-policies</pre>
msmtp	An SMTP client with a sendmail compatible interface.	<p>To configure msmtp, update msmtp.conf and provide an smtp host, username, password, and port.</p> <pre># msmtp recipient@domain.com</pre>
online-pg-backup	Allows you to take an online backup of the PostgreSQL database that contains Log Correlation Engine events and part of the Log Correlation Engine control state.	<p>For more information about online-pg-backup, see:</p> <ul style="list-style-type: none">• Perform an Online PostgreSQL Backup• Restore an Online PostgreSQL Backup
openssl-utils.sh	<p>Used to generate and view self signed CA certificates in .pem format when troubleshooting issues with Tenable Support.</p> <div>Note: This tool relies on the external openssl binary, not distributed with Log Correlation Engine but</div>	<pre>--generate-CA-creds <CA_dnSpec> <into_dir> [<certSpec>] (NB: any prior contents of <into_dir> will be erased!!) --generate-creds <hostSpec> <dnSpec> <into_ dir> <CA_creds_dir> [<certSpec>] (NB: any prior contents of <into_dir> will be erased!!) --is-signed-by <cert_path>.pem <CA_cert_ path>.pem --revoke <cert_path>.pem <CA_creds_dir> <CRL_ path>.pem --save-as-PKCS12 <endEntity_cert_path>.pem <endEntity_privkey>.pem <into_path>.pfx --print-cert <cert_path>.pem</pre>



Tool	Description	Usage
	<div>available as part of the OpenSSL RPM.</div> <div>Tip: This tool is intended for troubleshooting with Tenable Support. Otherwise, use the lce_crypto_utils tool.</div>	<pre>--print-CRL <CRL_path>.pem [<CA_cert_path>.pem] --print-PKCS12 <PKCS12_path>.pfx A <hostSpec> is: <host_DNS_name> <host_IP>; IP can be IPv4 or IPv6 A <dnSpec> is: , -separated list of K=V pairs, all optional save the last; \-escape as needed: 'C=<country>,ST=<state>,L=<city>,O=<org>,OU=<orgUnit>,CN=<name>' A <certSpec> is: <days_to_expiry> --rsa --dsa <bits>; defaults to: 366 --rsa 1024</pre>
optimize-datastore	<p>The PostgreSQL maintenance commands requisite for best query performance have been collected into the /opt/lce/tools/optimize-datastore script. It is suggested that you run this script during off-peak (low-load) hours, triggered by a cron(1) job. The contained commands are resource-intensive and query performance will be poor while optimize-</p>	<pre>(--only-silo <N> --all) [--also-cluster --also-reindex] [--max-runtime-hours <M>]</pre>



Tool	Description	Usage
	datastore is being run.	
<code>port-controlfiles</code>	<p>Allows you to save and restore all of an Tenable Log Correlation Engine server installation's control files, including:</p> <ul style="list-style-type: none">• policies• plugins• IDS signatures• cronjob definitions• SSH keys• daemon initscripts• Text search stopword lists <p><code>port-controlfiles</code> can be used to assist in moving an Tenable Log Correlation Engine instance from one host to another.</p>	<pre>--export --import <full path of previously exported .tar.gz></pre>



Tool	Description	Usage
query-plan-explainer	A convenient wrapper around the PostgreSQL EXPLAIN command, making its output both more concise and better readable.	<code>[--estimate-only] <sqlFile> "SQL query"</code>
send_syslog	Sends syslog messages to one or more servers.	<pre># /opt/lce/tools/send_syslog (server address 1) [...] [server address N] -message " (message)" [-port <port num>] [-priority #] [-facility <facility>] [-severity <severity>]</pre>
start-all	Starts PostgreSQL daemon and all Log Correlation Engine daemons.	<code># /opt/lce/tools/start-all</code>
restart-all	Without <code>bar-pg</code> , restarts the Log Correlation Engine daemons and PostgreSQL. With <code>bar-pg</code> , only restarts the Log Correlation Engine daemons.	<code># /opt/lce/tools/restart-all [bar-pg]</code>
stop-all	Without <code>bar-pg</code> , stops the Log Correlation Engine	<code># /opt/lce/tools/stop-all [bar-pg]</code>



Tool	Description	Usage
	daemons and PostgreSQL. With <code>bar-pg</code> , only stops the Log Correlation Engine daemons.	
<code>timestamp_formats.txt</code>	Used to identify the timestamp formats that appear for event timestamps in logs imported by <code>import_logs</code> . By default, this file includes a list of date formats.	If you are importing logs with timestamps in formats that are not included in this file, you can append the new formats to the list.
<code>toggle-augmented-event-lookups</code>	Tenable Log Correlation Engine Server maintains several special database lookups to improve query performance. These lookups incur a cost in [a] computing resources to build, and [b] disk space once built. If your queries involve the database column(s) to which a particular lookup is devoted,	<pre>--add-lookup --zap-lookup (rollup_table__ip rollup_table__port rollup_table__sensor rollup_table__user siloN_tables__event2 siloN_tables__ip siloN_tables__sensor siloN_tables__user)</pre>



Tool	Description	Usage
	<p>the benefit is well worth the cost; if not, disabling that lookup will save disk space.</p> <div>Note: Use only at direction of Tenable Support.</div>	
ts-test	Used to check how a particular log would be tokenized for the purpose of text search indexing and whether a particular text search phrase would match it.	<pre>[--detail-spaces] <rawDocument> [<tsQuery_inclStopwords>] or <path to file with rawDocument> [<tsQuery_inclStopwords>]</pre> <hr/> <p>To translate a showids +text search expression to a tsQuery expression, use /opt/lce/daemons/lce_queryd --translate-filter-on-rawlog <showidsSearchExpr></p> <p>For more information, see ts-test.</p>
validate-PRM-regex	To test matching, using exactly the same regex matching package, version, and settings, as used by the Tenable Log Correlation Engine engine.	<pre><PRM_reg.ex._line> <sample_log></pre> <p>For more information, see validate-prm-regex.</p>
user-utils	Reset the password	<pre>--list-all</pre>



Tool	Description	Usage
	for one of the secured accounts used to login to an Tenable Log Correlation Engine Server instance from outside the instance's host, if the Tenable Log Correlation Engine UI is for some reason unavailable or an operator simply prefers a console interaction for the purpose.	<pre>--lock--WebUI-acct <username> --unlock--WebUI-acct <username> --set-password--WebUI-acct <username> --replace--vuln_reporter-acct <username></pre> <p>Note: <code>--set-password--WebUI-acct</code> sets a temporary password and, if the user account was locked, unlocks the account.</p> <p>For more information about changing user passwords, see Change a User's Password. For more information about locked user accounts, see Locked User Accounts.</p> <p>Note: <code>--replace--vuln_reporter-acct</code> removes an existing account and sets a temporary password for the user. For more information about changing user passwords, see Change a User's Password.</p>



install-PostgreSQL-man-pages

This utility leverages the Linux man-page facility to provide a full local copy of official documentation for all PostgreSQL utilities and SQL commands; in the same format as native GNU/Linux utilities. They need to run only once, and then can issue commands such as:

Command	Description
<code>man 1 pg_dump,</code> <code>man 1 pg_restore</code>	Displays information about the PostgreSQL utilities for, respectively, export and import; these exact utilities are used by Tenable Log Correlation Engine's <code>archival-manager</code> utility.
<code>man 1 psql</code>	Displays information about the PostgreSQL command-line client (see also source-for-psql-shortcuts.sh .)
<code>man 1 pg_receivewal,</code> <code>man 1 pg_resetwal</code>	Displays information about PostgreSQL built-in clustering/replication facilities.
<code>man 7 SELECT</code>	Displays information about the complete syntax of the SQL <code>SELECT</code> command, including any PostgreSQL extensions to the SQL: 2011 (ISO/IEC 9075:2011) standard.
<code>man 7 CREATE_MATERIALIZED_VIEW</code>	Displays information about the complete syntax of the DDL <code>CREATE MATERIALIZED VIEW</code> command, including any PostgreSQL extensions to the SQL: 2011 (ISO/IEC 9075:2011) standard.
<code>man 7 CREATE_TEXT_SEARCH_CONFIGURATION,</code> <code>man 7 CREATE_TEXT_SEARCH_DICTIONARY,</code> <code>man 7 CREATE_TEXT_SEARCH_TEMPLATE</code>	Displays information about syntax of commands used to configure the PostgreSQL full-text search feature .



ts-test

The `ts-test` utility can tell you how PostgreSQL would parse a log and whether a given text search query matches that log.

Usage:

```
<rawDocument> [<tsQuery_inclStopwords>]
```

or

```
<path to file with rawDocument> [<tsQuery_inclStopwords>]
```

Example Output

If you invoke `ts-test` with a sample rawlog as the 1 arg, `ts-test` outputs a list of extracted terms and a detailed term extraction report table.

```
'The LCE agent at 192.0.2.10 [sensor: unknown] [type: networkmonitor  
v4.2.0.0] has been manually granted authorization to log in and send events  
to this LCE.'
```



Extracted terms					
'agent' 'authorization' 'granted' 'manually' 'networkmonitor' 'sensor' 'unknown' 'v4.2.0.0'					
Detailed term extraction report					
i	alias	description	token	dictionary	lexemes
1	asciiword	Word, all ASCII	The	human_language_rejecter	{}
2	asciiword	Word, all ASCII	LCE	whole_word_rejecter	{}
3	asciiword	Word, all ASCII	agent	simple	{agent}
4	asciiword	Word, all ASCII	at	human_language_rejecter	{}
5	version	Version number	172.26.28.10		
6	blank	Space symbols	[blanket_rejecter	
7	asciiword	Word, all ASCII	sensor	simple	{sensor}
8	blank	Space symbols	:	blanket_rejecter	
9	asciiword	Word, all ASCII	unknown	simple	{unknown}
10	blank	Space symbols] [blanket_rejecter	
11	asciiword	Word, all ASCII	type	whole_word_rejecter	{}
12	blank	Space symbols	:	blanket_rejecter	
13	asciiword	Word, all ASCII	networkmonitor	simple	{networkmonitor}
14	file	File or path name	v4.2.0.0	blanket_acceptor	{v4.2.0.0}
15	blank	Space symbols]	blanket_rejecter	
16	asciiword	Word, all ASCII	has	human_language_rejecter	{}
17	asciiword	Word, all ASCII	been	human_language_rejecter	{}
18	asciiword	Word, all ASCII	manually	simple	{manually}
19	asciiword	Word, all ASCII	granted	simple	{granted}
20	asciiword	Word, all ASCII	authorization	simple	{authorization}
21	asciiword	Word, all ASCII	to	human_language_rejecter	{}
22	asciiword	Word, all ASCII	log	whole_word_rejecter	{}
23	asciiword	Word, all ASCII	in	human_language_rejecter	{}
24	asciiword	Word, all ASCII	and	human_language_rejecter	{}
25	asciiword	Word, all ASCII	send	whole_word_rejecter	{}
26	asciiword	Word, all ASCII	events	whole_word_rejecter	{}
27	asciiword	Word, all ASCII	to	human_language_rejecter	{}
28	asciiword	Word, all ASCII	this	human_language_rejecter	{}
29	asciiword	Word, all ASCII	LCE	whole_word_rejecter	{}
30	blank	Space symbols	.	blanket_rejecter	

In this example output, the top two rows indicate the following:

- Token "The" was rejected by the `human_language_rejecter`.
- Token " " was rejected because our config rejects the entire "Space symbols" category.

Tip: Use the `--detail-spaces` option to show this information in the `ts-test` report.

- Token "LCE" was rejected by `whole_word_rejecter`.

If you provide a query string (for example, 'Authorization'), `ts-test` indicates whether that query string matches the sample rawlog:



```
./ts-test 'The LCE agent at 192.0.2.10 [sensor: unknown] [type:
networkmonitor v4.2.0.0] has been manually granted authorization to log in
and send events to this LCE.' 'Authorization'
```

```
Convert query to form w/o stopwords and punctuation
'authorization'
```

```
Testing match against converted query
Matched.
```

To see an example of match failure, provide a nonsense query string (for example, 'Bunnies?').

```
./ts-test 'The LCE agent at 192.0.2.10 [sensor: unknown] [type:
networkmonitor v4.2.0.0] has been manually granted authorization to log in
and send events to this LCE.' 'Bunnies?'
```

```
Convert query to form w/o stopwords and punctuation
'bunnies'
```

```
Testing match against converted query
Not matched.
```



validate-prm-regex

The `/opt/lce/tools/validate-PRM-regex` utility uses the same pattern matching library and parameters as the Log Correlation Engine engine. Tenable recommends using this tool to test your plugins.

`validate-PRM-regex` takes two arguments:

```
<PRM_reg.ex._line> <sample_log>
```

Note: As the `regex` argument, `validate-PRM-regex` accepts either an entire directive line (i.e. `regex=regexExpression` or `regexi=regexExpression`) exactly as it would appear in a `.prm` file; or just the *regexExpression*. In the latter case, it behaves as if *regexExpression* were prefixed by `regex=`.

Note: While you can and should feed `validate-PRM-regex` complete sample logs for final testing, log fragments are fine when developing.

Note: Enclose each argument in single quotes to protect from shell interpretation.

Example Output

Log Matched, Extracted 1 or More Substrings

```
validate-PRM-regex 'DstPort (\d{1,5}) ' 'with DstPort 55555 %'
```

```
Log matched, extracted 1 substring:
```

```
$1: [55555]
```

Log Matched, No Substrings Extracted

```
validate-PRM-regex 'DstPort \d{1,5} ' 'with DstPort 55555 %'
```

```
Log matched, no substrings extracted.
```

Tip: Enclose the subpattern you want to extract in parentheses to make it a capturing subpattern.



Log Not Matched

```
validate-PRM-regex 'DstPort (\d{1,5}) ' 'with DstPort % 55555'
```

```
Log not matched.
```

Invalid Regex

```
validate-PRM-regex 'DstPort (\d{1,5} ' 'with DstPort 55555 %'
```

```
Oct 22, 20 20:25 (validate-PRM-re) ERROR (plugins_regex.cpp:60,compile  
for validate-PRM-regex.cpp:78,main) - <:0> Compilation of the regex RE  
'DstPort ([0-9]{1,5} ' failed at char #10: missing )
```

```
Invalid regex.
```

Tip: The error message printed above may help to figure out what is wrong with the regex. In this example, exactly as the error message says, the closing delimiter) was missing.



Perform an Online PostgreSQL Backup

Caution: If you have configured high availability, do not perform an online backup at the standby node. For more information about high availability configurations, see [High Availability](#).

You can use the `online-pg-backup` utility to perform an online backup of the PostgreSQL that contains Log Correlation Engine events and part of the Log Correlation Engine control state. Online backups can be created while Log Correlation Engine and PostgreSQL are running.

The control state `online-pg-backup` saves does not include all control files, such as policies or plugins. To save all control files, use the [port-controlfiles](#) utility.

Before you begin:

- If this is the first time you are using the `online-pg-backup` utility, in the command line interface (CLI) in Log Correlation Engine, run the following command to restart PostgreSQL and all Log Correlation Engine daemons:

```
online-pg-backup --one-time-backup-prep
```

PostgreSQL and all Log Correlation Engine daemons restart.

To create an online PostgreSQL backup:

1. Log in to Log Correlation Engine via the command line interface (CLI).
2. In the CLI in Log Correlation Engine, run the following command:

```
online-pg-backup --backup-to <full path of directory>
```

PostgreSQL creates the backup files.

Note: This step may take 10-45 minutes to run, depending on the size of the backup file (10-20% of activeDb's size at the time backup was taken). Creating online backup files does not cause Log Correlation Engine or PostgreSQL downtime.

What to do next:

- (Optional) Restore the backup file, as described in [Restore an Online PostgreSQL Backup](#).



Restore an Online PostgreSQL Backup

Caution: If you have configured high availability, do not restore an online backup to the master node or the standby node. For more information about high availability configurations, see [High Availability](#).

You can use the `online-pg-backup` utility to restore an online PostgreSQL backup to a standalone Log Correlation Engine server node.

Note: Restoring an online backup completely replaces the PostgreSQL database. This may result in 10-45 minutes of downtime, depending on the size of the backup files.

Before you begin:

- Perform an online PostgreSQL backup, as described in [Perform an Online PostgreSQL Backup](#).

To restore an online PostgreSQL backup to a standalone Log Correlation Engine node:

1. Log in to Log Correlation Engine via the command line interface (CLI).
2. In the CLI in Log Correlation Engine, run the following command:

```
online-pg-backup --restore-from <full path of directory>
```

Log Correlation Engine restores the backup file.

PostgreSQL restarts.



Site Policies

You can specify the following site policies related to user activity using the `cfg-utils` utility:

- [Audit Log Policy](#)
- [Password Format Policy](#)
- [Password Reuse Policy](#)
- [Login Session Policy](#)

To configure a setting for any of the following policies, run:

```
/opt/lce/tools/cfg-utils --set-sv <configuration attribute> '<value>'
```

For more information about the `cfg-utils` utility and its usage, see [cfg-utils](#).

Audit Log Policy

You can configure the audit log policy to choose what user activities are logged, how often audit log backups are created, and whether the audit log is updated in real time.

You can view the complete audit log at any time by running `user-utils --print-audit-log`. For more information about the `user-utils` utility, see [user-utils](#).

By default, Tenable Log Correlation Engine tracks the following user activities in the audit log:

- account administration, such as adding and unlocking accounts
- session-scope actions with failure outcome, such as login failures or users logged out involuntarily

Configuration Attribute	Default	Description
web_UI__ account__audit_ session_ everything	false	If enabled, Tenable Log Correlation Engine tracks the following additional activities: <ul style="list-style-type: none">• session-scope actions with success outcome (logged in, logged out)



		<ul style="list-style-type: none">session tokens management actions (created token, destroyed token, ...)
<code>audit_log__ backup_ destination_ directory</code>	<i>none</i>	<p>If a directory is specified, Tenable Log Correlation Engine saves the entire audit log to a file every <code>audit_log__backup__interval__days</code> days.</p> <div>Note: The name of the audit log file includes the timestamp of when the file was created. For example: <code>/mnt/backups-nas/compliance/Tenable/LCE_Audit_Log__2020May27_00h31m02s.txt</code>.</div>
<code>audit_log__ backup_ interval__days</code>	<i>7</i>	<p>In days, sets how frequently Tenable Log Correlation Engine saves the audit file to the directory you specify using <code>audit_log__backup__destination__directory</code>.</p>
<code>audit_log__ notify_updates</code>	<i>false</i>	<p>If enabled, Tenable Log Correlation Engine writes each audit log entry to the host's syslog as it is created in real time. Site administrators can use this setting to receive notifications of new audit log entries.</p>

Password Format Policy

You can configure the password format policy to customize user password requirements.

Configuration Attribute	Default	Description
<code>web_UI__password__ minimum_length</code>	<i>4</i>	<p>Specifies the minimum number of characters that must be used when creating user passwords.</p>
<code>web_UI__password__ enforce_complexity</code>	<i>false</i>	<p>When enabled, user passwords must contain at least one of each of the following:</p> <ul style="list-style-type: none">An uppercase letterA lowercase letterA numerical characterA special character



Password Reuse Policy

You can configure the password reuse policy to specify how long passwords can be used, how frequently the same password can be reused, and how much new passwords must differ from previously-used passwords.

Configuration Attribute	Default	Description
web_UI__password__minimum_lifetime__hours	0	Specifies the number of hours a user must wait before changing their password after the last non-administrative password change. Note: Administrators can change another user's password at any time, regardless of this setting.
web_UI__password__max_lifetime__days	0	Specifies how frequently users must change their passwords. If a user has not changed their password before the specified number of days, the user account locks automatically. For more information, see Locked User Accounts .
web_UI__password__fewest_changes_ere_reuse	1	Specifies how frequently users can re-use the same password. By default, users cannot use the same password twice in a row. For example, if the value is set to 2, the user must use two other unique passwords before using the same password again.
web_UI__password__minimum_edit_distance	0	When set, requires new passwords to differ from previous passwords based on the edit distance value specified. New passwords must have at least x characters that differ from the previous password.

Login Session Policy

You can configure the login session policy to specify when user accounts are locked due to failed login attempts, set the maximum number of concurrent sessions per user, and set user accounts to be locked or logged out following a period of inactivity.



For more information about locked user accounts, see [Locked User Accounts](#).

Configuration Attribute	Default	Description
<code>web_UI__login__max_failures_during_window</code>	0	Specifies the number of times a user can attempt to log in during the window specified by <code>web_UI__login__failure_window_size__minutes</code> -minute before their account is locked.
<code>web_UI__login__failure_window_size__minutes</code>	15	Specifies the login window during which users will have <code>web_UI__login__max_failures_during_window</code> chances to try logging in before their account is locked.
<code>web_UI__login__max_concurrent_sessions</code>	5	Specifies the maximum number of concurrent login sessions per user.
<code>web_UI__account__lock_if_inactive__hours</code>	0	When set, Tenable Log Correlation Engine locks the account of any user who has not been active (logged in an interacting with the Tenable Log Correlation Engine web UI) in the specified number of hours.
<code>webserver__idle_session_timeout__minutes</code>	60	Specifies the number of minutes a user can be idle before being automatically logged out.

If `web_UI__login__max_failures_during_window > 0`, Tenable Log Correlation Engine will automatically lock (see <link to About Locked Accounts section>) the account of any user who has attempted but failed to log in `web_UI__login__max_failures_during_window` times in a `web_UI__login__failure_window_size__minutes`-minute period.



Rotate Web UI Credentials

You can use the `lce_crypto_utils` utility to rotate your user credentials for the Log Correlation Engine web UI. For more information about the `lce_crypto_utils` utility, see [lce_crypto_utils](#).

Note: These credentials only apply to users logging in the Log Correlation Engine web UI and not to uploading of vulnerability reports to Tenable Security Center.

To rotate web UI credentials:

1. Log in to Log Correlation Engine via the command line interface (CLI).
2. In the CLI in Log Correlation Engine, run the following command:

```
/opt/lce/credentials/web_UI/opt/lce/tools/lce_crypto_utils --generate-creds-webUI
```

Log Correlation Engine rotates your web UI credentials.



Encryption Strength

Tenable Log Correlation Engine uses the following default encryption for storage and communications.

Function	Encryption
Storing user account passwords	SHA-512 and the PBKDF2 function



Configure TLS Strong Encryption

You can configure TLS strong encryption for Log Correlation Engine-client communications to meet the security needs of your organization. Log Correlation Engine uses TLS 1.2 to encrypt Log Correlation Engine-client communications.

To configure TLS strong encryption for Log Correlation Engine communications:

1. Log in to Log Correlation Engine via the command line interface (CLI).
2. In the CLI in Log Correlation Engine, run the following command to specify the cipher you want to use for TLS encryption:

```
source /opt/lce/tools/exigent-sessions.bashrc
undoc-config --set lced cryptSyslog_ciphersuiteSelector <cipher you want to use
for TLS encryption>
```

For example:

```
source /opt/lce/tools/exigent-sessions.bashrc
undoc-config --set lced cryptSyslog_ciphersuiteSelector ECDHE-RSA-AES128-
SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES256-GCM-
SHA384
```

3. Run the following command to restart all Log Correlation Engine daemons:

```
restart-all bar-pg
```

All Log Correlation Engine daemons restart.



Configure Tenable Log Correlation Engine for NIAP Compliance

If your organization requires your instance of Log Correlation Engine to meet National Information Assurance Partnership (NIAP) standards, you can configure relevant settings to be compliant with NIAP standards.

You must run Log Correlation Engine 6.0.6 to configure Log Correlation Engine for NIAP compliance.

For more information about Log Correlation Engine storage and communications encryption, see [Encryption Strength](#). For more information about data gathered by the Log Correlation Engine Client, see [Tenable Log Correlation Engine Clients](#).

Before you begin:

- Confirm you have enabled the full disk encryption capabilities provided by the operating system on the host where Log Correlation Engine is installed.
- Contact Tenable Support for access to the following required script file:
 - LCE-NIAPcompliance-Oct29-fixerPkg.tgz

To configure Log Correlation Engine for NIAP compliance:

1. As the root user, in the command line interface (CLI) in Log Correlation Engine, run the following command to create a new directory for the script file:

```
mkdir /path/to/fixer29/
```

2. Run the following commands to download the script file into the directory you created:

```
cp /path/to/download/LCE-NIAPcompliance-Oct29-fixerPkg.tgz /path/to/fixer29
```

3. Run the following command to navigate to the `fixer29` directory:

```
cd /path/to/fixer29
```

4. Run the following command to extract the script:



```
tar xzf LCE-NIAPcompliance-Oct29-fixerPkg.tgz
```

5. Run the following command to start LCE-NIAPcompliance-Oct29-fixer:

```
./LCE-NIAPcompliance-Oct29-fixer
```

6. Run the following commands to enable NIAP-compliant settings:

```
. /opt/lce/tools/exigent-sessions.bashrc  
enable_NIAP_Mode
```

Log Correlation Engine restarts.

Log Correlation Engine secures communications with TLS 1.2 and the following cipher suites: ECDHE-RSA-AES128-SHA256, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES256-SHA384, or ECDHE-RSA-AES256-GCM-SHA384.

Note: Enabling NIAP mode encrypts communications for the following:

- Receiving the encrypted TCP syslog. For more information, see [Receiving Encrypted Syslog](#).
- Sending vulnerability reports to Tenable Security Center.
- Downloading plugin updates.
- Web UI server and desktop browser.

7. (Optional) Run the following commands to view your NIAP settings and enabled cipher suites:

```
undoc-config --get wwwd NIAP_COMPLIANT
```

8. If you connect Log Correlation Engine to Tenable Security Center, you must use certificates to authenticate the connection. For more information, see [Manual Key Exchange with Tenable Security Center](#).



File and Process Allow List

If you use third-party endpoint security products such as anti-virus applications and host-based intrusion and prevention systems, you should add Log Correlation Engine to the allow list.

The following tables list the Log Correlation Engine Server and Log Correlation Engine Client folders, files, and processes that should be allowed.

Log Correlation Engine Server

Log Correlation Engine Server
Folders
/opt/lce/*
/opt/lce/admin/log/*
/opt/lce/db/*
/tmp/*
/tmp/download_surge_domains
/tmp/download_surge_files
/tmp/user_tracking_day
/tmp/sw_tracking_day
/tmp/threatlist.tmp
/tmp/threaturl.tmp
/tmp/usb_tracking_day
/etc/logrotate.d/lce
/etc/keepalived/keepalived.conf
/etc/sysconfig/keepalived
/etc/systemd/system/keepalived.service



/usr/lib/systemd/system/keepalived.service
/var/run/keepalived
/usr/lib/firewalld/services/lce-server.xml
/etc/init.d/
/var/lock/subsys/
Files
/opt/lce/tools/optimize-datastore
/opt/lce/tools/cache-filter-pointers
/opt/lce/diag
/opt/lce/showids
/opt/lce/tasl
/opt/lce/daemons/lce_client_manager
/opt/lce/postgresql/bin/pg_basebackup
/opt/lce/postgresql/bin/pg_ctl
/opt/lce/postgresql/bin/pg_dump
/opt/lce/postgresql/bin/pg_isready
/opt/lce/postgresql/bin/pg_restore
/opt/lce/postgresql/bin/pg_rewind
/opt/lce/postgresql/bin/psql
/opt/lce/tools/archival-manager
/opt/lce/tools/check_fix-file_accessibility
/opt/lce/tools/cfg-utils
/opt/lce/tools/fwd-silo-cksum



/opt/lce/tools/ha-manager
/opt/lce/tools/msmtp
/opt/lce/tools/restart-all
/opt/lce/tools/send_syslog
/opt/lce/tools/start-all
/opt/lce/tools/stop-all
/opt/lce/tools/user-utils
Processes
/opt/lce/daemons/lced
/opt/lce/daemons/lce_queryd
/opt/lce/daemons/lce_report_proxyd
/opt/lce/daemons/lce_wwwd
/opt/lce/daemons/lce_tasld
/opt/lce/daemons/stats
/opt/lce/postgresql/bin/postgres
/opt/lce/ha/keepalived

Log Correlation Engine Clients

Tenable NetFlow Monitor
Folders
/opt/netflow_monitor/
/etc/init.d/netflow_monitor
Processes



tfmd

Tenable Network Monitor

Folders

(Linux only) /opt/network_monitor/

(FreeBSD only) /usr/local/network_monitor

/etc/init.d/network_monitor

Processes

tnmd

OPSEC Client

Folders

/opt/lce_opsec/*

/etc/init.d/lce_opsec

Files

lce_query_opsec

Processes

lce_opsecd

Tenable RDEP Monitor

Folders

/opt/rdep_monitor/

/etc/init.d/rdep_monitor

Processes

trm

Tenable SDEE Monitor



Folders

/opt/sdee_monitor/

/etc/init.d/sdee_monitor

Processes

Ice_sdeed

Splunk Client

Folders

/opt/lce_splunk/

/etc/init.d/lce_splunk

Processes

Ice_splunkd

Log Correlation Engine Client for Linux

Folders

(FreeBSD only) /usr/local/lce_client/

/opt/lce_client/

(OSX only) /Library/LaunchDaemons/com.tenable.launchd.lceclient.plist

(AIX only) /etc/rc.d/init.d/lce_client

(HP-UX only) /sbin/init.d/lce_client

/etc/init.d/lce_client

Processes

Ice_clientd

Log Correlation Engine Client for Windows

Folders



C:\Program Data\Tenable\LCEClient
C:\Program Files\Tenable\LCEClient
Files
server_assignment.exe
Processes
lce_client.exe
Web Query Client
Folders
/opt/lce_webquery/*
/etc/init.d/lce_webquery
Processes
lce_webqueryd
WMI Monitor Agent
Folders
/opt/wmi_monitor/*
/etc/init.d/wmi_monitor
Files
wmi_config_credentials wmic
Processes
lce_wmid



Refresh or Replace the Vulnerability Reporter SSL Certificate

Required User Role: Administrator

To update the self-signed SSL certificate used to upload vulnerability reports to Tenable Security Center, do one of the following:

- Rotate the self-signed SSL certificate, replacing it with a fresh self-signed certificate.
- Replace the self-signed SSL certificate packaged with Log Correlation Engine with an SSL certificate from your organization.

To rotate the self-signed SSL certificate and replace it with a fresh self-signed certificate:

1. Log in to Log Correlation Engine via the command line interface (CLI).
2. In the CLI in Log Correlation Engine, run the following command to refresh the SSL certificate:

```
/opt/lce/tools/lce_crypto_utils --generate-creds-vulnReporter -q
```

Log Correlation Engine regenerates the SSL certificate locally.

3. Re-add the Log Correlation Engine to Tenable Security Center, as described in [Add a Tenable Log Correlation Engine Server](#) in the *Tenable Security Center User Guide*.

To replace the SSL certificate used to upload vulnerability reports to Tenable Security Center:

1. Copy the following files from your CA to `/opt/lce/reporter/ssl/`.
 - cacert.pem
 - servercert.pem
 - cakey.pem
 - serverkey.pem

Note: Do not change the certificate file names.



2. Add the Log Correlation Engine to Tenable Security Center, as described in [Add a Tenable Log Correlation Engine Server](#) in the *Tenable Security Center User Guide*.



Import Log Correlation Engine Data Manually

Log Correlation Engine data can be collected both via real-time logging and manually in batch mode using the **import_logs** tool. These events will show up in the normalized event view along with events collected in real-time. This command-line tool allows data to be imported into the Log Correlation Engine that may not be available in real-time, but is still important for correlation of vulnerability data and for analysis of security posture and events.

Log files must be in ASCII format or UTF8, not binary, and each log must be delimited by a single newline.

Note: Event silos in the Log Correlation Engine activeDb may not overlap in respective time spans of contained events.

Usage:

```
# /opt/lce/tools/import_logs
--ASCII | --UTF8
[--now-as-timestamp | --may-guess-timestamps]
[--minimum-timestamp-epoch <N>]
[--maximum-timestamp-epoch <N>]
[--no-eval-event-rules]
<inputFileAbsolutePath>
```

The following table describes the options available for **import_logs**:

Option	Description
--no-eval-event-rules	Do not apply Log Correlation Engine event rules to imported logs.
--may-guess-timestamps	If no timestamp can be determined for an event, assign the most recent known timestamp.
--now-as-timestamp	Use the current system time for all imported logs rather than the timestamps contained within the event text.



Manual Key Exchange with Tenable Security Center

A manual key exchange between Tenable Security Center and the Log Correlation Engine is normally not required; however, in some cases where remote root login is prohibited or key exchange debugging is required, you will need to manually exchange the keys.

For the remote Log Correlation Engine to recognize Tenable Security Center, you need to copy the SSH public key of Tenable Security Center and append it to the `/opt/lce/.ssh/authorized_keys` file on the Log Correlation Engine server. The `/opt/lce/daemons/lce-install-key.sh` script performs this function.

Note: The Log Correlation Engine server must have a valid license key installed and the Log Correlation Engine daemon must be running before performing the steps below.

To manually exchange the keys with Tenable Security Center:

1. In Tenable Security Center, download the Tenable Security Center key, as described in [Download the Tenable Security Center SSH Key](#) in the *Tenable Security Center User Guide*. Both DSA and RSA formats work for this process.
2. Save the key file (SSHKey.pub) to your local workstation. Do not edit the file or save it to any specific file type.
3. From the workstation where you downloaded the key file, use a secure copy program, such as “scp” or “WinSCP” to copy the SSHKey.pub file to the Log Correlation Engine system. You will need to have the credentials of an authorized user on the Tenable Log Correlation Engine server to perform this step. For example, if you have a user “bob” configured on the Log Correlation Engine server (hostname “lceserver”) whose home directory is `/home/bob`, the command on a Linux or Unix system would be as follows:

```
# scp SSHKey.pub bob@lceserver:/home/bob
```

4. After the file is copied to the Log Correlation Engine server, in the command line interface (CLI), run the following command to move the file to `/opt/lce/daemons`:

```
# mv /home/bob/SSHKey.pub /opt/lce/daemons
```



5. On the Log Correlation Engine server, as the root user, run the following command to change the ownership of the SSH key file to "lce":

```
# chown lce /opt/lce/daemons/SSHKey.pub
```

6. Run the following command to append the SSH public key to the "/opt/lce/.ssh/authorized_keys" file:

```
# su lce
# /opt/lce/daemons/lce-install-key.sh /opt/lce/daemons/SSHKey.pub
```

7. To test the communication, as tns user on the Tenable Security Center system, attempt to run the `id` command:

```
# su tns
# ssh -C -o PreferredAuthentications=publickey lce@<LCE-IP> id
```

- If a connection has not been previously established, you will see a warning similar to the following:

```
The authenticity of host '192.168.15.82 (192.168.15.82)' can't be
established. RSA key fingerprint is
86:63:b6:c3:b4:3b:ba:96:5c:b6:d4:42:b5:45:37:7f. Are you sure you
want to continue connecting (yes/no)?
```

Answer "yes" to this prompt.

- If the key exchange worked correctly, a message similar to the following will be displayed:

```
# uid=251(lce) gid=251(lce) groups=251(lce)
```

8. You can add the IP address of Tenable Security Center to the Log Correlation Engine system's `/etc/hosts` file. This prevents the SSH daemon from performing a DNS lookup that can add seconds to your query times.



9. Add the Log Correlation Engine to Tenable Security Center, as described in [Add a Tenable Log Correlation Engine Server](#) in the *Tenable Security Center User Guide*.



User Tracking

The Tenable Log Correlation Engine server has a feature that is designed to track users. User tracking can be applied to any event coming into the Tenable Log Correlation Engine server, regardless of the source of the event. Events correlated from Windows, Linux, Unix, or other network devices can be monitored.

When Tenable Log Correlation Engine encounters a log that has no username field, it will assign the username of the user most recently associated with the source IP of the incoming log, or associated with the destination IP of the log if a destination IP (dstip) is provided but a source IP (srcip) is not. If no user was previously tracked at either of the IPs, or if no IP is provided, an “(unknown)” entry is assigned.

When a user changes IP addresses (i.e., a Tenable Log Correlation Engine receives a log where the user’s srcip differs from the srcip in the previous log tagged with the username), the new IP address is also associated with the user. The last three IP addresses per user are stored for the user, allowing for cases where a single user logs into multiple systems at the same time. For example, the following event shows a user becoming active at a new IP address:

```
Network user IP address change: user someguy94 became active at 169.254.96.232 with
event login (169.254.96.232:0)
```

The data used to track usernames is stored in the files `usernames.txt`, `ip_user.dat`, and `user_ip.dat` in the Tenable Log Correlation Engine database directory. The `.dat` files are written when the Tenable Log Correlation Engine service is shut down gracefully. In case of a server crash, the data is automatically backed up every 10 minutes.

A maximum of 65,534 unique usernames can be stored. If the maximum is reached, incoming logs with new users will have the user fields marked with the “(unknown)” entry.

User tracking in Tenable Log Correlation Engine will function if the following conditions are met:

- The Tenable Log Correlation Engine server has plugins that can match the events and pull usernames from the events. For example, plugin 3209 in `os_win2k_sec.prm` has the following line:



```
log=event:Windows-Account_Used_For_Login sensor:$1 dstip:$2 type:login
user:$4 event2:WindowsEvent-680
```

The `user:$4` directive tells the plugin to add the username to the available event searchable fields. As a result, searches that query this event based on the username will return results.

- The plugin IDs have been added to the **User Tracking Plugins** in the **User Tracking** section in the configuration section of the Tenable Log Correlation Engine interface (one plugin ID per line).

Note: A list of the plugins provided by Tenable that include user information is found at the end of `/opt/lce/daemons/plugins/prm_map.prm`.

- The user tracking settings have been properly configured in the Tenable Log Correlation Engine interface under “User Tracking”. Please refer to the Advanced Configuration Options section of this document for a description of the following applicable keywords:
 - `accept-letters`
 - `accept-numbers`
 - `additional-valid-characters`
 - `max-username-characters`

If these conditions are not met, usernames may still be stored in normalized events; however, they cannot be searched using the event filter **username** parameter. Another way to search for usernames in logs is through the raw log search feature of Tenable Security Center.



Non-Tenable License Declarations

Below you will find the command that will list all the third-party software packages that Tenable provides for use with the Tenable Log Correlation Engine. This command may be run at the command line interface by users with permissions to the lced binary.

```
# /opt/lce/daemons/lced -l
```

For a list of third-party software packages that Tenable utilizes with Log Correlation Engine, see [Tenable Log Correlation Engine Third-Party Licenses](#).



Silo Archiving

Configuration

- Total size of activeDb is limited by config attribute `active-size` (default: 20 TB).
- Total size of archiveDb is limited by config attribute `archive-size` (default: 20 TB).

Control Flow

Every 2.5 minutes, Tenable Log Correlation Engine will:

1. Read in the results of the last-executed action, from Tenable Log Correlation Engine status database.
2. Choose the next action to take based on the last-executed action.
3. Perform the next action and store results in Tenable Log Correlation Engine status database.

Storing the state in this manner has the following advantages:

- simplicity (no separate logic to handle reloads/restarts is needed)
- transparency (to see exactly where the archival algorithm is, just query the Tenable Log Correlation Engine status database.)
- available emergency override (can alter the control flow by updating the Tenable Log Correlation Engine status database.)

Note: This is not standard operating procedure and should only be performed in very rare cases.

Tenable Log Correlation Engine waits a maximum of 60 minutes for an archive job to complete in order to avoid being stuck in the `CheckArchiveDone` state indefinitely in the rare case that PostgreSQL fails to report an archive job as complete.

Note: Archiving a silo normally takes 6 to 8 minutes.

Example `archival-manager --list-snapshots` Output



(2020Nov09 17:33:34 - 2020Nov09 20:01:28)	silos-1604961214-1604970088-42974973-recordLive
4.0GB Compress= 7 Written= 2020Dec13 16:44:11 Can "peek"= yes	
(2020Nov09 15:06:15 - 2020Nov09 17:33:33)	silos-1604952375-1604961213-42999973-recordLive
4.1GB Compress= 4 Written= 2020Nov14 09:24:36 Can "peek"= yes	
(2020Nov10 14:02:43 - 2020Nov13 20:17:25)	silos-1605034963-1605316645-28282397-recordLive
1.3GB Compress= 4 Written= 2020Nov13 20:23:09 Can "peek"= yes	
(2020Nov09 12:36:34 - 2020Nov09 15:06:14)	silos-1604943394-1604952374-43148821-recordLive
4.1GB Compress= 4 Written= 2020Nov10 13:07:34 Can "peek"= yes	
(2020Nov09 10:26:54 - 2020Nov09 12:36:33)	silos-1604935614-1604943393-38125839-recordLive
3.7GB Compress= 4 Written= 2020Nov09 19:25:15 Can "peek"= yes	
(2020Nov08 19:13:32 - 2020Nov09 10:26:53)	silos-1604880812-1604935613-43086813-recordLive
4.1GB Compress= 4 Written= 2020Nov09 16:59:19 Can "peek"= yes	