tenable network security

# Log Correlation Engine 4.6 Quick Start Guide

January 25, 2016

(Revision 2)

# Table of Contents

# Introduction

This document provides basic instructions for installing and configuring Tenable Network Security's Log Correlation Engine (LCE) version 4.6or newer. This is not intended to be a comprehensive document on the product and is only focused on essential steps needed to get the product up and running. Please refer to additional documentation available on the Tenable Support Portal for more information. Please email any comments and suggestions to support@tenable.com.

Familiarity with system log formats from various operating systems, network devices, and applications and a basic understanding of Linux/Unix command line syntax is also assumed.

## Standards and Conventions

Throughout the documentation, filenames, daemons and executables are indicated with a **courier bold** font such as **gunzip**, **httpd**, and **/etc/passwd**.

Command line options and keywords are also indicated with the **courier bold** font. Command line examples may or may not include the command line prompt and output text from the results of the command. Command line examples will display the command being run in **courier bold** to indicate what the user typed while the sample output generated by the system will be indicated in courier (not bold). Following is an example running of the Linux/Unix **pwd** command:

```
# pwd
/opt/lce/daemons
#
```

Important notes and considerations are highlighted with this symbol and grey text boxes.

Tips, examples, and best practices are highlighted with this symbol and white on blue text.

## Product Overview

Tenable's Log Correlation Engine helps organizations find and respond to security threats and demonstrate compliance with policies and regulatory requirements.

The Log Correlation Engine collects, normalizes, and analyzes logs from devices throughout your network. It analyzes and correlates data from firewalls, intrusion detection and prevention systems, and data loss prevention solutions, as well as raw network traffic, application logs and user activity logs.

## Prerequisites

Tenable recommends a minimum of 4 GB of memory and a Dual-Core 3.0GHz processor. Disk space is recommended to be approximately 1.5 times the size of the license. A storage configuration of SAS 3 Gb/s, RAID 0 striping is recommended. LCE is available for Red Hat Enterprise Server 5 (64-bit), 6 (64-bit), and 7 (64-bit). CentOS 5 (64-bit), 6 (64-bit), and 7 (64-bit) are also officially supported. For more information on hardware requirements for your environment, please review the Log Correlation Engine 4.6 High Availability Large Scale Deployment Guide and Tenable General Requirements Guide.

# LCE Quick Start

This document refers to three primary LCE components: the LCE Client (the device that initially collects data and sends it on to the LCE server); the LCE server (or daemon), which is installed on Red Hat/CentOS and performs the bulk of the processing; and SecurityCenter, which provides a graphical user interface to view and report on the LCE data.

## Installation

### System Prerequisites

- A RHEL/CentOS 5, 6, or 7 platform with all unnecessary services disabled
- LCE license file (you will need the output of the "**`hostname`**" command to obtain a license file)
- An Activation Code
- SecurityCenter Continuous View. For more information, visit: http://www.tenable.com/products/securitycenter/securitycenter-continuous-view.
- Firewall configuration:
  - Open 514/UDP for standard syslog
  - Open 601/TCP for reliable syslog
  - Open 443/TCP for remote access to the LCE Manager web console if installed on the same server
  - Open 31300/TCP for LCE client/server communications
  - Open 31302/TCP for LCE server load balancing (when used)
  - Open 6514/TCP for encrypted syslog(if required)

These ports cannot be used by any other processes. For example, the **`syslogd`** service on 514/UDP or 601/TCP must be disabled, or set to listen on different ports.

### Prepare the Activation Code

The free, demo, or commercial activation code must obtained before proceeding. A commercial activation code can be obtained by logging into https://support.tenable.com. After the initial installation is complete, navigate to the DNS name or the IP address of the LCE server over port 8836 (https://<dns name or IP address>:8836>) in your preferred web browser.

### Dependencies

Although it is possible to force the installation without all required dependencies, if your version of Red Hat or CentOS is missing certain dependencies, this will cause problems that are not readily apparent with a wide variety of functions. Tenable's Support team has observed different types of failure modes for SecurityCenter when dependencies to the installation RPM are missing. If you require assistance or guidance in obtaining these dependencies, please contact Tenable's Support team at support@tenable.com.

The following programs must be installed on the system prior to installing the LCE server:

- coreutils
- initscripts
- perl
- gawk
- net-tools
- procps
- openssh-clients
- gzip
- findutils
- openssl
- bind-utils
- wget
- rsync

Always use the latest stable production version of each package approved by your IT department. Depending on initial OS installation options, other packages may be requested during product installation.

To determine which version is on your system, run the following command for each of the packages (replace "**libxslt**" with the appropriate package):

```
# rpm –qa | grep libxslt
```

If one of the prerequisite packages is missing, it can be installed using the "yum" or "rpm" package managers. For example, to install Java 1.7.0 and answer "yes" to all questions, use "yum" with the command below:

```
# yum -y install java-1.7.0-openjdk.i386
```

## Install the LCE Server Package

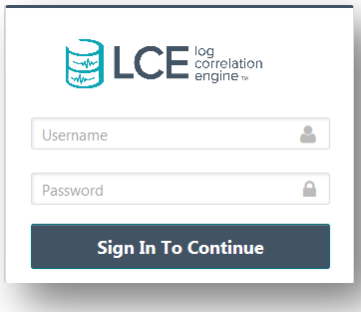
As the root user, install the LCE Server RPM using the following command:

```
# rpm -ivh lce-4.x.x-es6.i386.rpm
```

The "Setup Wizard" is used to complete the basic setup of LCE 4.6. Each step of the "Setup Wizard" is shown in the section below.

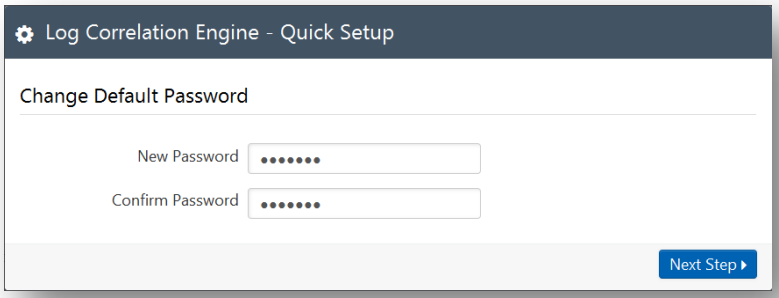
### *Setup Wizard*

After the initial installation is complete, navigate to the DNS name or the IP address of the LCE server over port 8836 (https://<dns name or IP address>:8836>) in your preferred web browser. The login screen will be displayed. The default login credentials are User name "admin" and password "admin". Enter the default information, and select "Sign In To Continue".



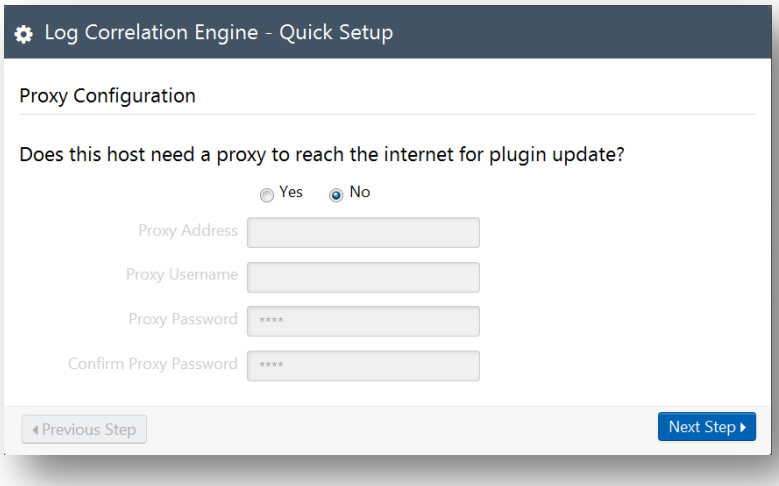

## Step 1: Change Default Password

Upon initial login, the "Quick Setup" will begin. The first step is to change the password. The password complexity is set to 4 alphanumeric characters. The password complexity can be changed, and will be covered in a later section of this guide.



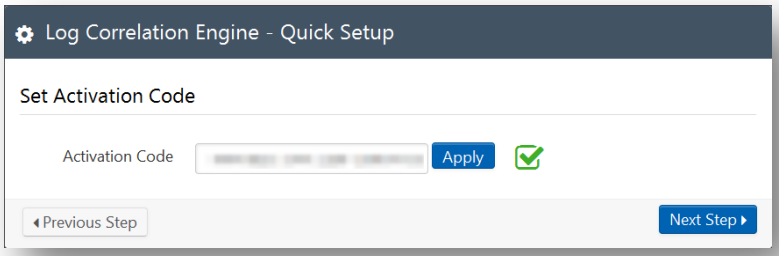

## Step 2: Proxy Configuration

The next section of the configuration wizard requires "Proxy Configuration" information. If a proxy is utilized in the environment where LCE is deployed select "Yes" and enter the required information into the corresponding fields. If a proxy is not required, select "No". After the appropriate option is selected and any corresponding fields are completed, choose "Next Step".



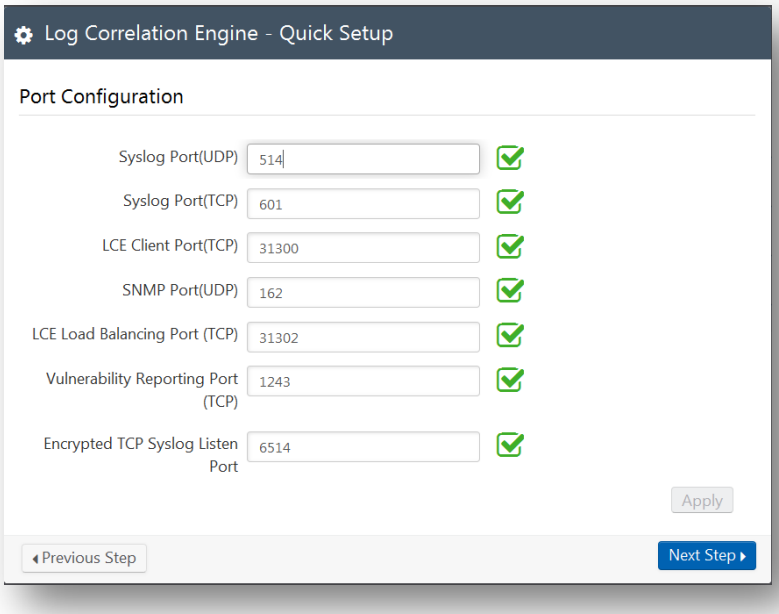
### Step 3: Set Activation Code

The "Set Activation Code" section requires a valid activation code. The activation code can be obtained by logging into the Tenable Support Portal (https://support.tenable.com) and then selecting "Activation Codes". Enter the Activation Code and click "Apply". A check mark can be seen next to the "Apply" button to confirm the activation code is valid. When the activation code has been entered correctly, select "Next Step" to proceed. If the LCE is not connected to the Internet, an offline plugin update will need to be periodically performed. Please review the Offline Activation and Plugin Update section of this guide for more information.



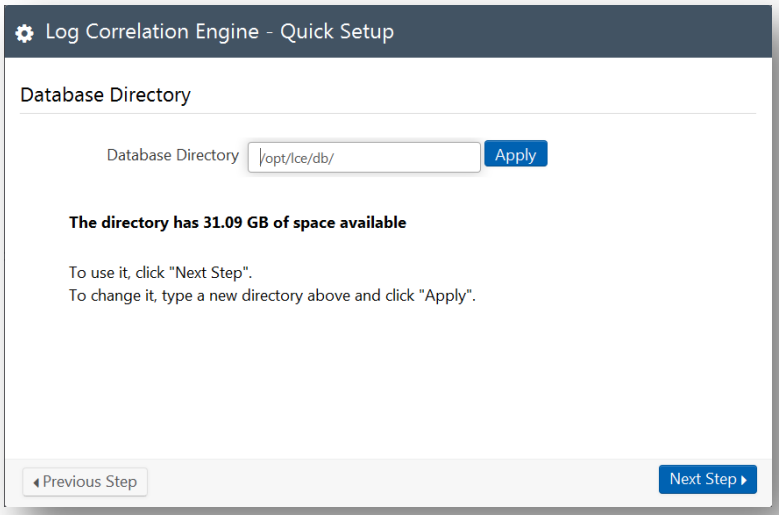

### Step 4: Port Configuration

The "Port Configuration" section displays the default ports already assigned for each type of communication. If an alternate port is used for communication for the services listed, it can be changed here. If changes are made, select "Apply" to ensure those changes are enforced. Then select "Next Step" to continue.



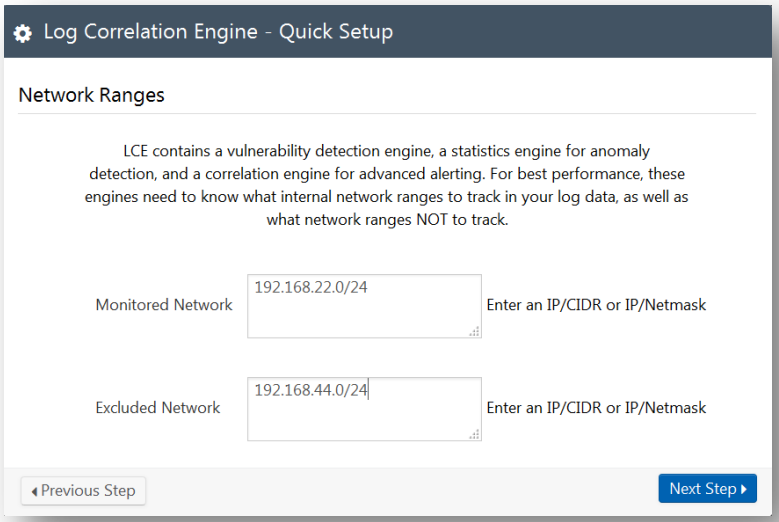
## Step 5: Database Directory

The “Database Directory” section displays the default LCE database location, “**`/opt/lce/db/`**”. This can be changed to an alternate directory if needed, but is not recommended. If it is changed after the “Quick Setup” is complete, the database will need to be moved using a manual process. If changes are made, select “Apply” to ensure those changes are enforced. Confirm that there is adequate space available in the directory location for the license that you have uploaded, which is reported in the center of the “Database Directory” window, and then select “Next Step” to continue.



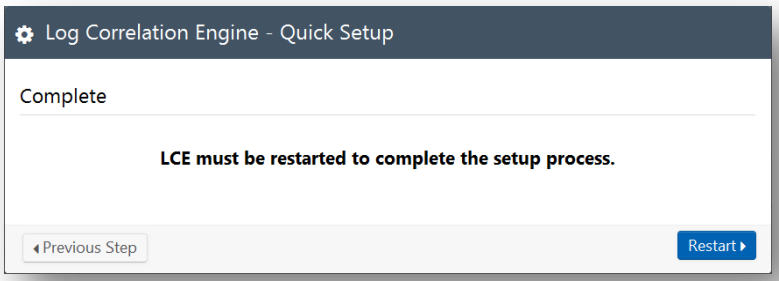

## Step 6: Network Ranges

The “Network Ranges” section specifies the networks to be monitored or ignored by LCE. The network ranges that are to be monitored by LCE will need to be entered in CIDR notation (192.168.0.0/24) or IP/netmask (192.168.0.0/255.255.255.0) into the “Monitored Network” box. The networks that are excluded from LCE will need to be entered in CIDR notation or IP/Netmask in the “Excluded Network” box. After the information is entered select “Next Step”.



### Setup Complete

At this point the "Quick Setup" process is complete, and LCE services will require a restart. If you would like to revisit any step before finalizing the configuration, choose "Previous Step" to edit the desired step. Otherwise select "Restart" to complete setup.




Once the LCE has restarted, the initial configuration is complete. It is possible to log in to the LCE web interface to address any additional configuration to include syslog forwarding, load balancing across multiple LCE servers, NAT setup for LCE clients, and other advanced settings.

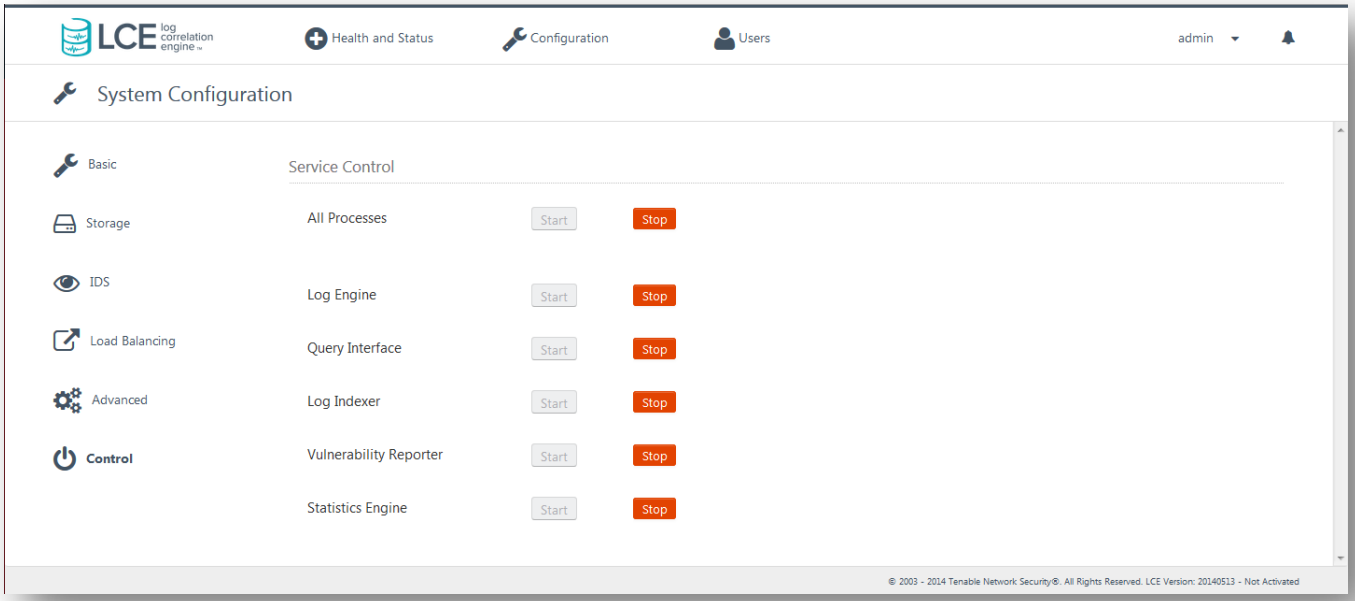
For more information on large scale deployments, please refer to the Log Correlation Engine 4.6 High Availability Large Scale Deployment Guide.

The installation process will create a user and group named "**lce**" and install the LCE server to the **/opt/lce** directory. All files will be installed with the user and group of "lce" except for the actual **lced** daemon, which is set-user-id root. This must be started as the "root" user, and once the daemon has bound to the appropriate port(s), it will drop privileges. If the **lced** daemon terminates abnormally for any reason, the system will automatically restart the daemon and add a warning to the LCE logs.

LCE provides many options that can be fine-tuned to suit a wide variety of environments. Since this document focuses on getting LCE up running as quickly as possible, only the options that are prompted by the setup wizard are noted. Please refer to the LCE documentation noted at the end of this document for more information on available options.

## Basic LCE Server Operations

The LCE 4.6 has the ability to control each LCE service via the LCE GUI. The "Control" section of "System Configuration" is used to verify the status of an LCE service. This section can also be used to start and stop each service that is related to LCE if needed.




| Option | Description |
|---|---|
| All Processes | "Stop" or "Start" all LCE daemons |
| Log Engine | "Stop" or "Start" the LCE daemon |
| Query Interface | "Stop" or "Start" the LCE query daemon |
| Log Indexer | "Stop" or "Start" the LCE indexer daemon |
| Vulnerability Reporter | "Stop" or "Start" the LCE Vulnerability Reporter daemon |
| Statistics Engine | "Stop" or "Start" the Statistics daemon |

## LCE Clients

The LCE Client is installed on hosts to monitor and collect events that are forwarded on to the LCE server daemon. When received by the LCE server, events are stored both as raw logs as well as normalized and correlated with vulnerabilities (if applicable). The SecurityCenter UI makes both the raw and normalized event data available to the user for event and analysis and mitigation.

The LCE supports many types of agents including:

- Windows Event Logs (collected locally or remotely via WMIC)
- Windows/Linux/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
- File monitoring (Linux, Unix and Windows)

LCE has many signature processing libraries to parse logs and can normalize and correlate most network Intrusion Detection System (IDS) devices, as well as messages from SecurityCenter. The LCE supports the following IDS sources:

## IDS Collection and Correlation

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

TippingPoint's **syslog** event format must be modified to use a comma delimiter instead of a tab delimiter before it can be processed by the LCE.

## IDS Collection Only

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

The list of officially supported log sources is frequently updated on the Tenable web site's LCE product page.

## Installing the Linux Clients

To install the LCE Client, obtain the package for your OS platform and desired client and install as the *root* user on the target client system.

The following table provides an installation example for some of the available LCE Clients on supported platforms. Any special installation instructions are provided in a note following the example.

| LCE Client | Installation Example |
|---|---|
| **Red Hat** | |
| LCE Log Agent | `# rpm -ivh lce_client-4.x.x-esX.i386.rpm` |
| LCE WMI Monitor Agent | `# rpm -ivh wmi_monitor-4.x.x-esX.i386.rpm` |
| Tenable NetFlow Monitor | `# rpm -ivh TenableNetFlowMonitor-4.x.x-esX.i386.rpm` |

| | |
|---|---|
| Tenable Network Monitor | `# rpm -ivh TenableNetworkMonitor-4.x.x-esX.i386.rpm` |

A successful installation is indicated by the return of the command prompt with no errors.

## Linux Client Configuration

Once the client is installed, the LCE Server IP address and LCE Server Port will need to be set using the **set-server-ip.sh** script. For this example, both LCE client and LCE server are on the same system, so we can use the localhost IP address of 127.0.0.1, and the default LCE server port of 31300. When the process is complete, the LCE client daemon will restart (see below).

```
# /opt/lce_client/set-server-ip.sh

Enter the new desired LCE server IP or hostname.
>>
127.0.0.1


Enter the new desired LCE server port [31300].
>>
31300
Updating LCE Server IP from 203.0.113.1 to 127.0.0.1...
Updating LCE Server Port from 31300 to 31300...
Done

Stopping LCE Client daemon                                 [  OK  ]
Starting LCE Client daemon                                 [  OK  ]
```

| LCE Client | Configuration File |
|---|---|
| **Red Hat** | |
| LCE Log Agent | `/opt/lce_client/set-server-ip.sh` |
| LCE WMI Monitor Agent | `/opt/wmi_monitor/set-server-ip.sh` |
| Tenable NetFlow Monitor | `/opt/netflow_monitor/set-server-ip.sh` |
| Tenable Network Monitor | `/opt/network_monitor/set-server-ip.sh` |

## Controlling the Linux Client

Below is a table that displays how to start, stop, and restart the client software on the various platforms:

| LCE Client | Methods (start/stop/restart) |
|---|---|
| **Red Hat** | |
| LCE Log Agent | `# service lce_client {start\|stop\|restart\|status}` |
| LCE WMI Monitor Agent | `# service wmi_monitor {start\|stop\|restart\|status}` |
| Tenable NetFlow Monitor | `# service netflow_monitor {start\|stop\|restart\|status}` |
| Tenable Network Monitor | `# service network_monitor {start\|stop\|restart\|status}` |

## Windows Client Configuration

The Log Correlation Engine Windows Log Agent client monitors events, as well as specific log files or directories, for new event data. Tenable currently provides two Windows LCE Log Agents: one for Windows XP/2003 platforms and one for Windows Vista/2008/7 platforms.

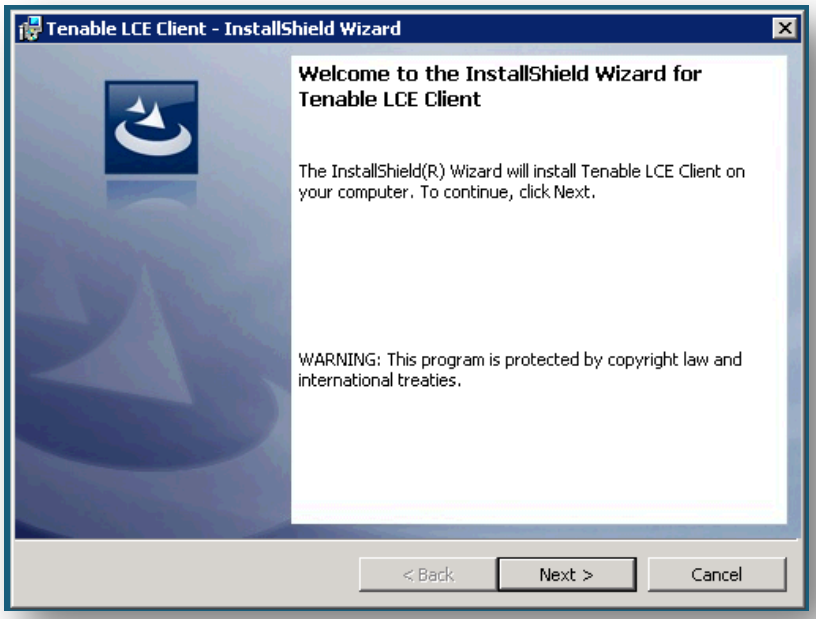
| Platform | LCE Client Type | Install File Name and Utility |
|---|---|---|
| **MS Windows XP Professional, Windows Server 2003** | LCE Log Agent | `lce_client-4.x.x-windows_2003_x86.msi` |
| **MS Windows Server 2008, 2012 Windows Vista, Windows 7, 8** | LCE Log Agent | `lce_client-4.x.x-windows_2008_x86.msi`<br>`lce_client-4.x.x-windows_2008_x64.msi` |

## Installing the Windows Client

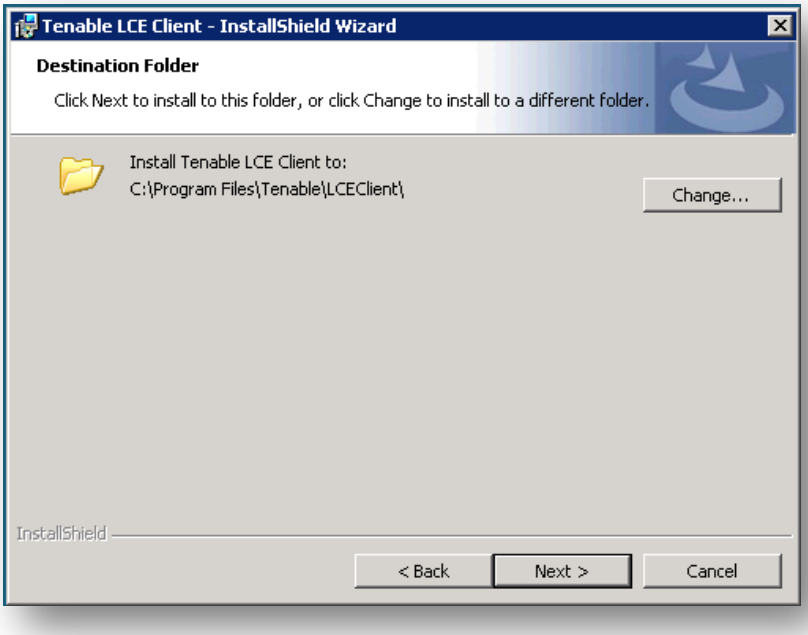
The LCE Windows Log Agent client is installed by clicking on the `.msi` distribution file, which will launch the InstallShield Wizard. On machines where Universal Access Control (UAC) is enabled, the user must run the installer as an Administrator level user. Right-click the installer icon and select "**Run as Administrator**".

The windows LCE client requires .NET 4.0 to install successfully.

A license agreement will be displayed that must be agreed to before installation can continue. The installer will prompt to choose if the application is to be shared or not, as shown in the following screen:




Click "**Next**".



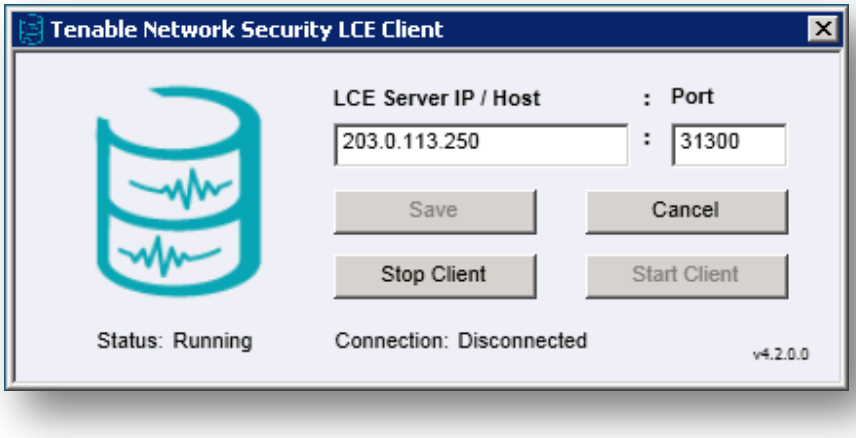

To use the default location, simply click "**Next**" and a screen will be displayed to begin the installation by clicking "**Install**". After a short period, the InstallShield Wizard will display a screen indicating that the installation is complete. Once installation is complete, you may be prompted to restart the system for the configuration changes to take effect.

### Windows Client Configuration

To configure the LCE Windows Log Agent client, launch the LCE Configuration tool located at "**`C:\Program Files\Tenable\LCEClient\LCE_Server_Assignment.exe`**". Depending on options selected during installation, a shortcut icon(s) is created on the Desktop and the "**Start**" menu under "**Tenable Network Security**" called "**LCE Client Configuration**".

The only configuration required is the LCE server IP address or DNS name and the port (if the server is configured for one other than the default of 31300). All other configuration options will be managed by the LCE Client Manager upon connection.

An example screen for the LCE Client Configuration tool is shown below:




By default, the LCE Log Agent client is configured using a non-routable documentation IP address (203.0.113.250) and LCE Server Port 31300. These settings must be changed to the IP address or hostname and listening port of the actual LCE server. No further local configuration is required. Once set, select the "**Save**" button followed by "**Start Client**".

Once the client connects to the LCE server and is authorized by the LCE Client Manager, the appropriate configuration file will be pushed to the client.

## SecurityCenter Configuration

Please refer to the "Log Correlation Engines" section of the "SecurityCenter 5.0 Administration Guide" for details on how to add LCE to SecurityCenter.

# For More Information

Tenable has produced a variety of other documents detailing the LCE's deployment, configuration, user operation, and overall testing. These documents are listed here:

- Log Correlation Engine Architecture Guide – provides a high-level view of LCE architecture and supported platforms/environments.
- Log Correlation Engine 4.6 Administrator and User Guide – describes installation, configuration, and operation of the LCE.
- Log Correlation Engine 4.6 Quick Start Guide – provides basic instructions to quickly install and configure an LCE server. A more detailed description of configuration and management of an LCE server is provided in the "LCE Administration and User Guide" document.

- Log Correlation Engine 4.4 Client Guide – how to configure, operate, and manage the various Linux, Unix, Windows, NetFlow, and other clients.
- Log Correlation Engine 4.4 OPSEC Client Guide – how to configure, operate, and manage the OPSEC Client.
- Log Correlation Engine 4.6 High Availability Large Scale Deployment Guide – details various configuration methods, architecture examples, and hardware specifications for performance and high availability of large scale deployments of Tenable's Log Correlation Engine (LCE).
- Log Correlation Engine Best Practices – Learn how to best leverage the Log Correlation Engine in your enterprise.
- Tenable Event Correlation – outlines various methods of event correlation provided by Tenable products and describes the type of information leveraged by the correlation, and how this can be used to monitor security and compliance on enterprise networks.
- Tenable Products Plugin Families – provides a description and summary of the plugin families for Nessus, Log Correlation Engine, and the Passive Vulnerability Scanner.
- Log Correlation Engine Log Normalization Guide – explanation of the LCE's log parsing syntax with extensive examples of log parsing and manipulating the LCE's `.prm` libraries.
- Log Correlation Engine TASL Reference Guide – explanation of the Tenable Application Scripting Language with extensive examples of a variety of correlation rules.
- Log Correlation Engine 4.4 Statistics Daemon Guide – configuration, operation, and theory of the LCE's statistic daemon used to discover behavioral anomalies.
- Example Custom LCE Log Parsing - Minecraft Server Logs – describes how to create a custom log parser using Minecraft as an example.

Documentation is also available for Nessus, the Passive Vulnerability Scanner, and SecurityCenter through the Tenable Support Portal located at https://support.tenable.com/.

There are also some relevant postings at Tenable's blog located at http://www.tenable.com/blog and at the Tenable Discussion Forums located at https://discussions.nessus.org/community/lce.

For further information, please contact Tenable at support@tenable.com, sales@tenable.com, or visit our web site at http://www.tenable.com/.

## About Tenable Network Security

Tenable Network Security provides continuous network monitoring to identify vulnerabilities, reduce risk, and ensure compliance. Our family of products includes SecurityCenter Continuous View™, which provides the most comprehensive and integrated view of network health, and Nessus®, the global standard in detecting and assessing network data. Tenable is relied upon by many of the world's largest corporations, not-for-profit organizations and public sector agencies, including the entire U.S. Department of Defense. For more information, visit tenable.com.

# Appendix 1: Offline Activation and Plugin Updates

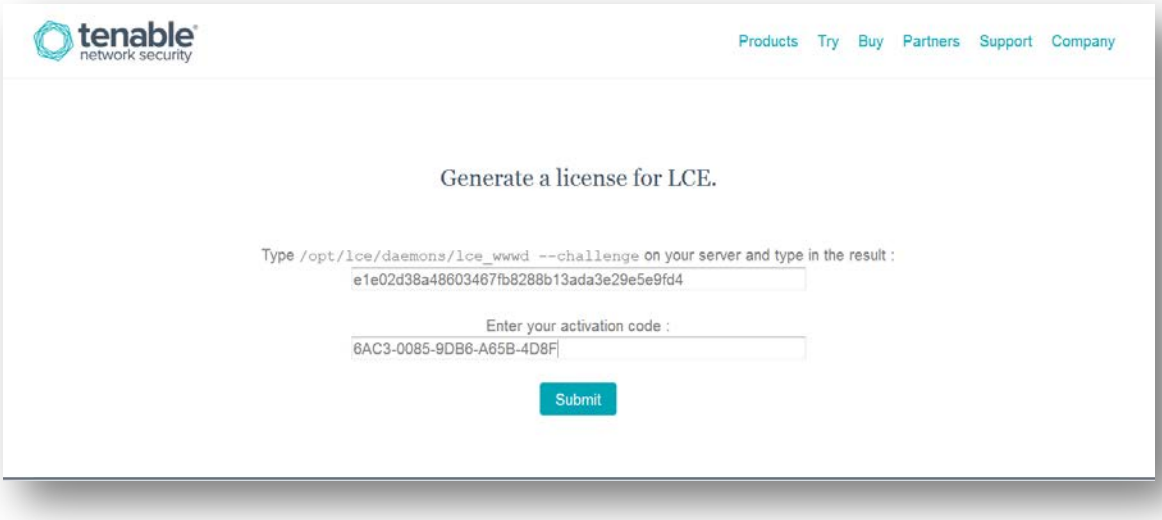
The steps below explain how to activate and update LCE plugins on an air gapped network.

## Offline Activation

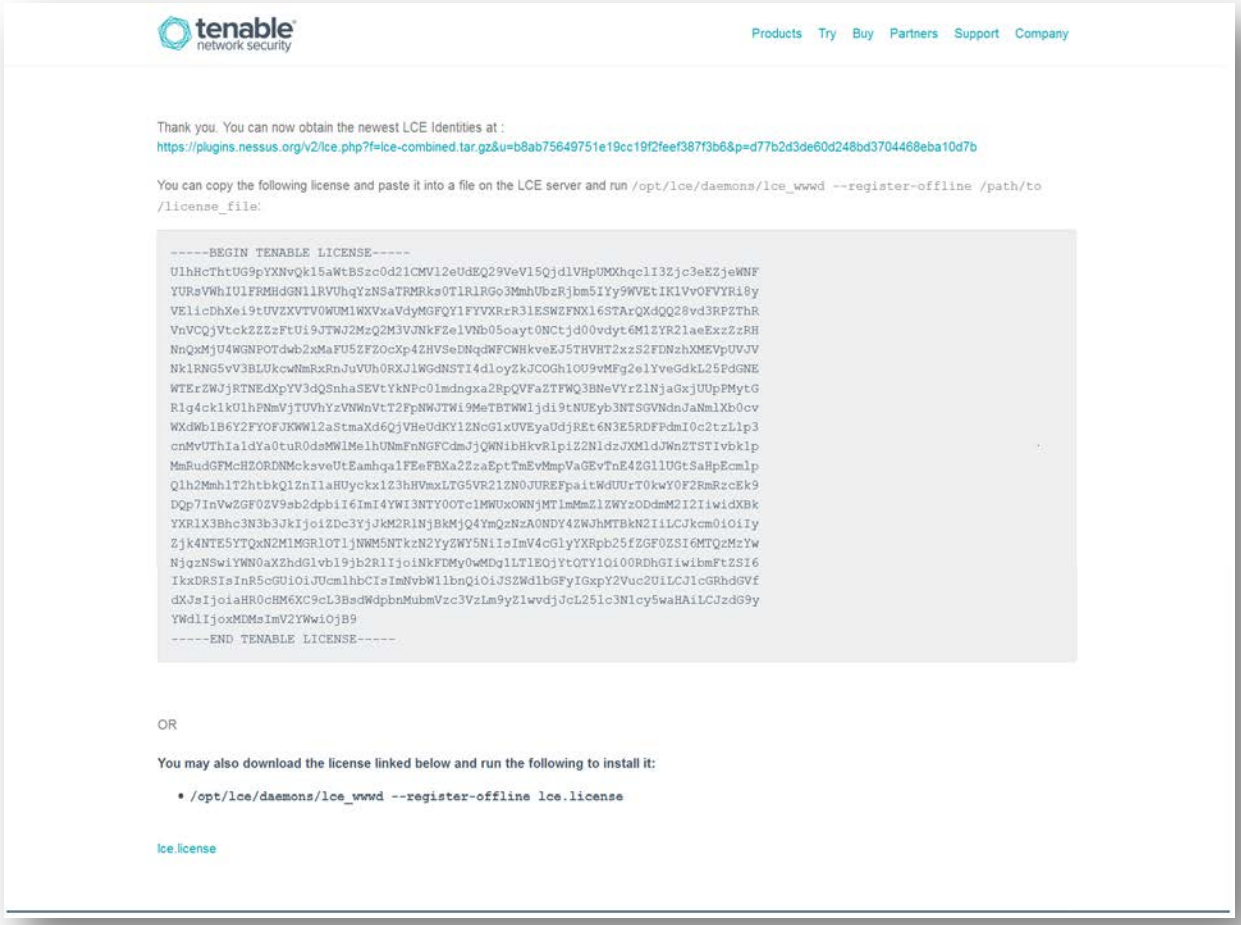
1. Navigate to https://support.tenable.com and log in.
2. Select "Activation Codes" from the menu, and select the plus symbol (+) next to "Log Correlation Engine," then copy the "Activation Code" to be used with the offline LCE.
3. Log in to the offline LCE terminal as root user, and execute the command below.

```
# /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
```

4. Using a web browser, go to https://plugins.nessus.org/v2/offline-lce.php and enter the challenge activation and codes obtained in the previous steps.




5. Select the link that is generated to download the current plugin set. Make a copy of the link that is returned. The link provided will be valid until the LCE subscription expires. Save the link, as it will be needed each time the plugins are manually updated.



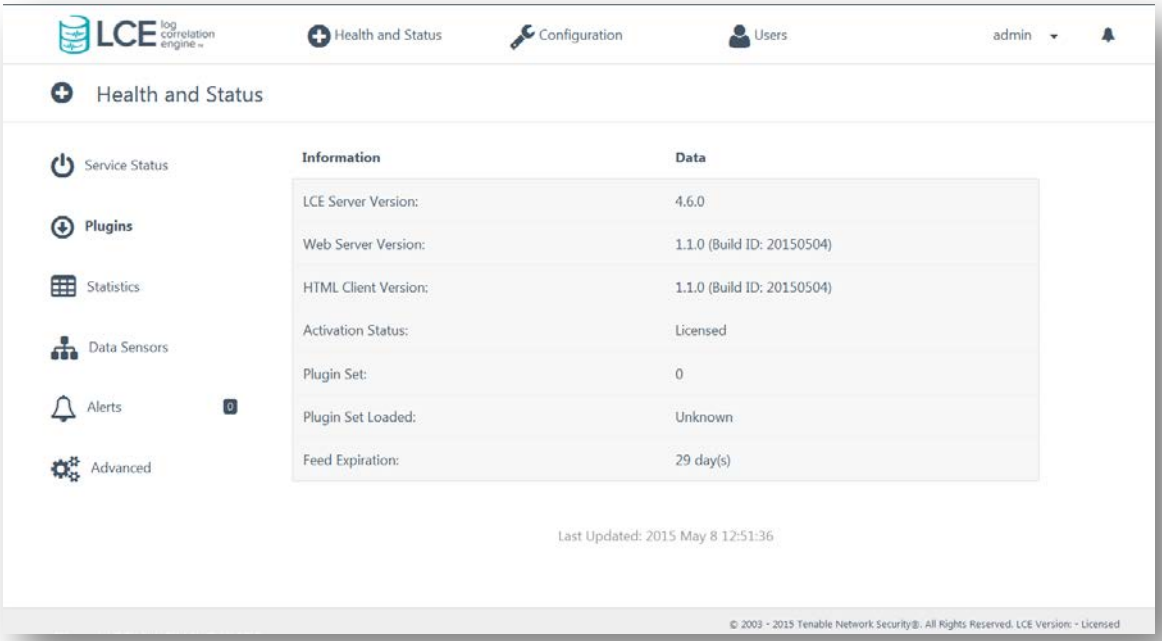

6. Select the link to download the license key "**`lce.license`**", or create a **`lce.license`** file by copying the information returned into a text file from "-----BEGIN TENABLE LICENSE-----" to "-----END TENABLE LICENSE-----".

7. Upload the **`lce.license`** file to **`/opt/lce/daemons`**, and run the following command:

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

8. Navigate to https://<ip address of your lce>:8836 and complete the setup and configuration steps above.

9. To verify the license has been loaded successfully, choose "Health and Status" followed by "Plugins". The "Activation Status" should now show "Licensed" as shown in the image below.




## Offline Plugin Updates

1 Using the link found in step 5 of the "Activation" section, download the newest "**`lce-combined.tar.gz`**" file

2 Under the "Offline Plugin Update" section, choose "Browse" to upload the "**`lce-combined.tar.gz`**" file. The "**`lce-combined.tar.gz`**" file contains updates for LCE PRM(s), TASL(s), discoveries, client policies, the web client, and the web server. After the file is uploaded successfully, choose "Process Plugins". The process may take a minute or two to complete.

3 To verify the plugins have been loaded successfully, choose "Health and Status" followed by "Plugins". The "Plugin Set" and the "Plugin Set Loaded" will now be populated as shown in the image below.