LCE Windows Client 5.0 User Guide

Last Revised: April 24, 2018

Table of Contents

Getting Started **3**

Standards and Conventions 4

Hardware Requirements 5

System Requirements 6

Licensing 7

Install, Configure, and Remove **8**

Download an LCE Client 9

Install the LCE Windows Client 10

Install the LCE Windows Client Remotely 11

Configure the LCE Windows Client 13

Remove the LCE Windows Client 14

LCE Windows Client Features **16**

How To **17**

Configure the Windows Client Policy 18

Reference **19**

Authorize an LCE Client 20

Assign a Policy to an LCE Client 21

Client Policy Builder 22

Create a Client Policy with the Client Policy Builder 24

Edit a Client Policy with the Client Policy Builder 27

Clone a Client Policy with the Client Policy Builder 30

Windows Client Policy Configuration Items 34

Getting Started

This document describes the LCE Client version 5.0 for Windows that is available for Tenable Network Security's Log Correlation Engine. This documentation refers to the LCE Client for Windows as the "LCE Windows Client."

A working knowledge of Secure Shell (SSH), Log Correlation Engine (LCE), and SecurityCenter Continuous View (SecurityCenter CV) operation and architecture is assumed. Familiarity with general log formats from various operating systems, network devices, and applications as well as a basic understanding of Microsoft Windows is also assumed.

Please email any comments and suggestions to support@tenable.com.

Overview

The LCE Windows Client monitors events, as well as specific log files or directories, for new event data. Tenable Network Security provides 32-bit and 64-bit versions of the LCE Windows Client for Windows Server 2008/Server 2012/7/8/10 platforms.

Standards and Conventions

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

Command line options and keywords are also indicated with the **bold monospace** 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 **bold monospace** to indicate what the user typed while the sample output generated by the system will be indicated in **monospace** (not bold). Following is an example running of the Unix **pwd** command:

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

Note: Important notes and considerations are highlighted with this color.

Tip: Tips, examples, and best practices are highlighted with this color.

Caution: Crucial information the user must know. For example, *The LCE server daemon will restart following this operation.*

Hardware Requirements

Hardware	Minimum Requirement
Processor	Dual Core x86-64
Processor Speed	2 Ghz
Ram	2 GB
Disk Space	100 MB

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 2008/2012/2012 R2/2016, Windows Vista/7/8/10 - 64-bit

Additional Software

The Windows Client requires the following software:

- LCE 5.0.x
- Microsoft Visual C++ 2015 Redistributable Package, Update 2

Licensing

SecurityCenter CV must be licensed to utilize the LCE Windows Client.

Install, Configure, and Remove

This section includes the following instructions for installing, configuring, and removing the LCE Windows Client. With the exception of downloading the Windows Client, the following procedures must be performed on the command line.

- Download the LCE Windows Client
- Install the LCE Windows Client
- Install the LCE Windows Client Remotely
- Configure the LCE Windows Client
- Remove the LCE Windows Client

Download an LCE Client

Steps

1. Access the Tenable Support Portal.

   The **Tenable Customer Support Portal** page appears.

2. On the left side of the page, in the **Main Menu** box, click the **Downloads** link.

   The **Tenable Download Center** page appears.

3. Click the **Log Correlation Engine** link.

   The **Log Correlation Engine Download** page appears.

4. At the top of the page, in the list of products, click the link that corresponds to the LCE client that you want to download, and then select the appropriate version for your operating system.

   The **Software License Agreement** appears.

5. Review the Software License Agreement. If you agree to the terms, click the **I accept the terms of this license** button.

   The client package is downloaded.

Install the LCE Windows Client

In addition to installing the LCE Windows Client locally, you can also install the LCE Windows Client on remote hosts.

Before You Begin

Download the LCE Windows Client.

Steps

1. If you are installing the LCE Windows Client on a host where User Account Control is enabled, right-click the LCE Windows Client .msi file and select **Run As Administrator**. Otherwise, double-click the LCE Windows Client .msi file.

   The LCE 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 LCE Client is installed.

Install the LCE Windows Client Remotely

The installation of the LCE 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 LCE 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 LCE Windows Client MSI install package. Because all parameters (except LCE 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 LCE server. The maximum length of the hostname is 46 characters. If not specified, the value is set to *203.0.113.250*.
SERVERPORT	The port used to communicate with the LCE server. The default port is *31300*.

Caution: Versions of the LCE Windows Client earlier than 4.4 also provided the SERVERNAME property. That property is deprecated and should not be used.

Before You Begin

Download the LCE Windows Client.

Steps

1. Using a script or via the command line, execute the following: `msiexec.exe /qn /i "<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 LCE server that you want the LCE 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 LCE server. Specify an integer between 1 and 65535. The default port is *31300*.

The **/qn** in the executed command instructs the .msi file to run with no user feedback. When performing an installation from the command line, the **/qn** option can be used to keep the installation program from stopping the process to ask if previous settings should be applied. If desired, the **/passive** option can be used in place of **/qn**, which will display the progress of the installation, but it doesn't allow for user interaction.

The **/i** is the operative parameter that specifies the name of the file to be installed.

If a log file of the installation is desired, **/l** can be used, followed by the path to the log file. For example: `msiexec.exe /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: `msiexec.exe /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 .msi file.

Configure the LCE Windows Client

If you did not configure the LCE Windows Client during installation, or if you want to modify the configuration, you can configure the client using the command line.

Steps

1. Via the command line, go to the directory where you installed the LCE Windows Client, and then execute the following command: `server_assignment.exe --server-ip "<Server IP or Hostname>" --server-port <Server Port>`

    - **<Server IP or Hostname>** corresponds to the IP address or hostname of the LCE server that you want the LCE 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 LCE server. The default port is *31300*.

2. Type `net stop "Tenable LCE Client"`

    The Tenable LCE Client service stops.

3. Type `net start "Tenable LCE Client"`

    The Tenable LCE Client service starts. The LCE Windows Client is configured.

Note: After the client is configured and authorized by the LCE 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.

Remove the LCE Windows Client

The LCE Windows Client can be removed in three ways:

- Using the original .msi file that you installed the Windows Client with.
- Using the command line.
- Using the Control Panel for your version of Windows. 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.

Remove Using the LCE Windows Client .msi File

1. If you are removing the LCE Windows Client from a host where User Account Control is enabled, right-click the LCE Windows Client .msi file and select **Run As Administrator**. Otherwise, double-click the LCE 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 LCE 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 LCE Client service must be stopped in order for the removal to complete successfully. By default, the Tenable LCE Client service will be stopped.

5. If you do not want to stop the Tenable LCE 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 LCE Windows Client is removed.

Remove Using the Command Line

1. Via the command line, execute the following: `msiexec.exe /qn /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.

The **/qn** in the executed command instructs the .msi file to run with no user feedback.

LCE Windows Client Features

The LCE 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 LCE server for normalization. In the case of monitored text files, each new line is transmitted. After the LCE server normalizes the event data, the data can be visualized using SecurityCenter Continuous View. The LCE 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 LCE server as an event. When unknown processes are monitored, you can configure the LCE 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 LCE 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 LCE 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 LCE server as events. When malware scanning is enabled, the LCE Windows Client will use DNS queries to compare the MD5 checksums.

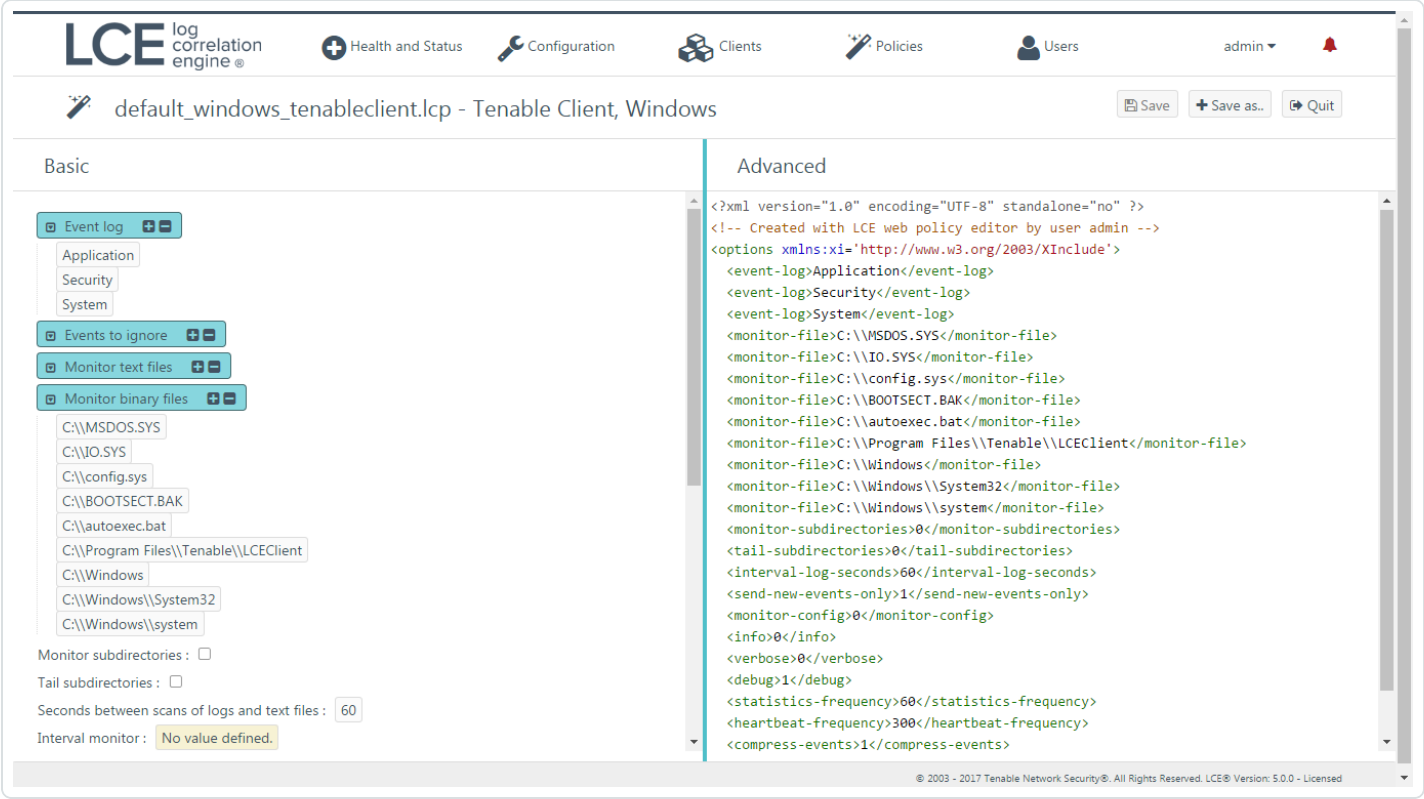
How To

This section contains the following topics:

- Configure the Windows Client Policy

Configure the Windows Client Policy

Using the Client Policy Builder, you can create and modify policies for your LCE Windows Client. The following steps are performed via the web interface on the LCE server that you configured your LCE Windows Client to communicate with.



Steps

1. Using the Client Policy Builder, create a policy for your LCE Windows Client. This documentation includes a list of valid configuration items for the client policy.
2. Assign the policy to the LCE Windows Client.

Reference

This section contains the following topics:

- Authorize an LCE Client
- Assign a Policy to an LCE Client
- Client Policy Builder
- Windows Client Policy Configuration Items

Authorize an LCE Client

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

Steps

1. In the top navigation bar, click **Clients**.

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

2. In the client table, in the rows corresponding to the LCE clients that you want to authorize, select the check boxes.

   > **Tip:** You can use filters or sort by the **Authorized** column to quickly find LCE clients that need to be authorized.

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

   The **Authorize** dialog box appears.

4. Review the list of LCE clients that will be authorized, and then click the **Authorize** button.

   The LCE clients are authorized and will immediately send a heartbeat.

Assign a Policy to an LCE Client

In addition to using SecurityCenter and the **Policies** page, you can assign policies to LCE clients via the **Clients** page.

Steps

1. In the top navigation bar, click **Clients**.

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

2. In the client table, in the row corresponding to the LCE client that you want to assign a policy, select the check box.

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

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

   The **Change policy** dialog box appears.

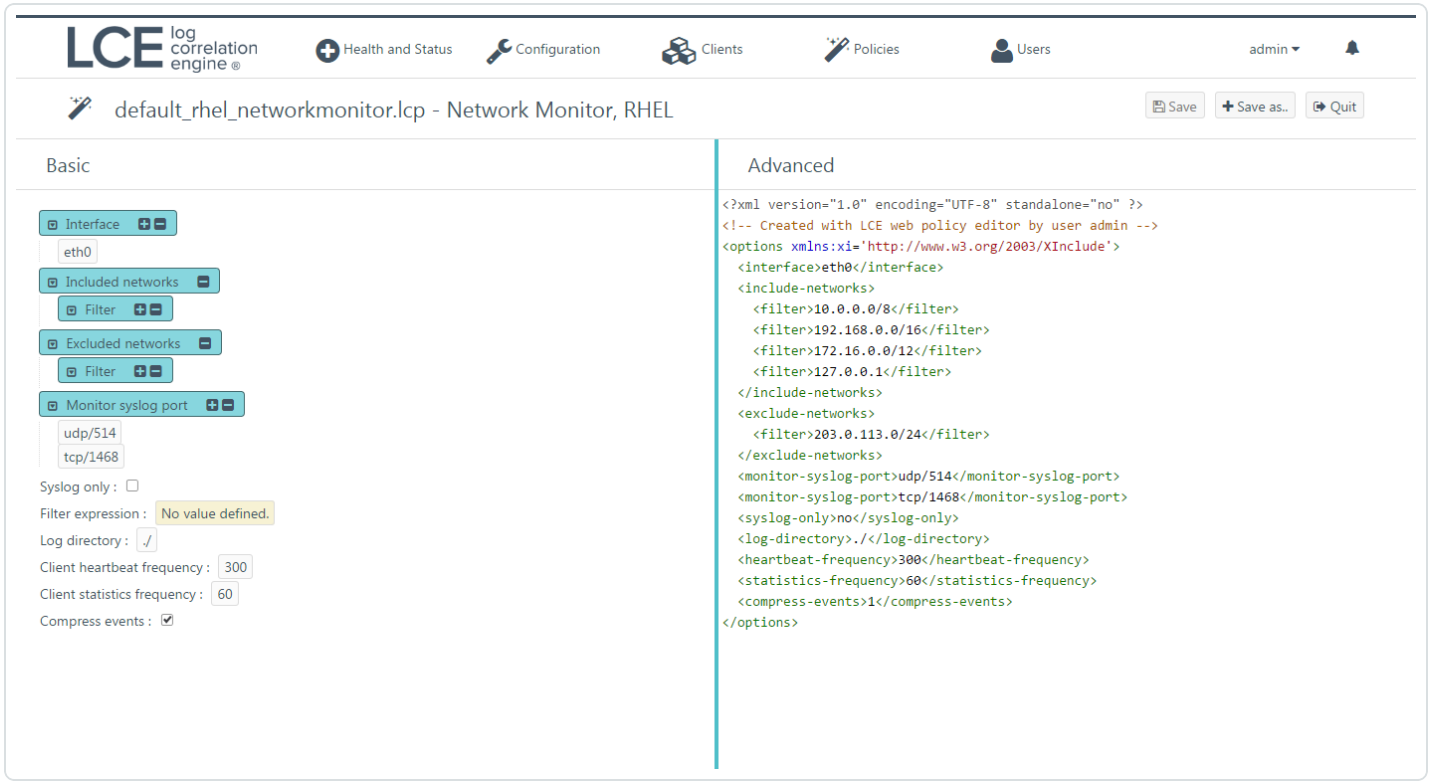
4. In the **Assign the following policy** list, select the policy that you want to assign to the LCE client.

5. Review the LCE client that will have a new policy, and then click the **Change policy** button.

   The specified policy is assigned to the LCE client.

Client Policy Builder

The Client Policy Builder is a tool for creating and editing policies directly in the LCE interface. The Builder can be used to create a policy for any supported combination of LCE 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 LCE, the Builder can be used to modify any existing policies and will alert you if an existing policy that you modify is invalid.



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

The title bar appears at the top of the Builder and displays the file name of the policy. If you are creating a new policy, the default name will reflect the LCE client type and the operating system that the policy supports. Additionally, the title bar contains the **Save**, **Save as..**, and **Quit** buttons.

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.

Primarily, the Builder will be used to:

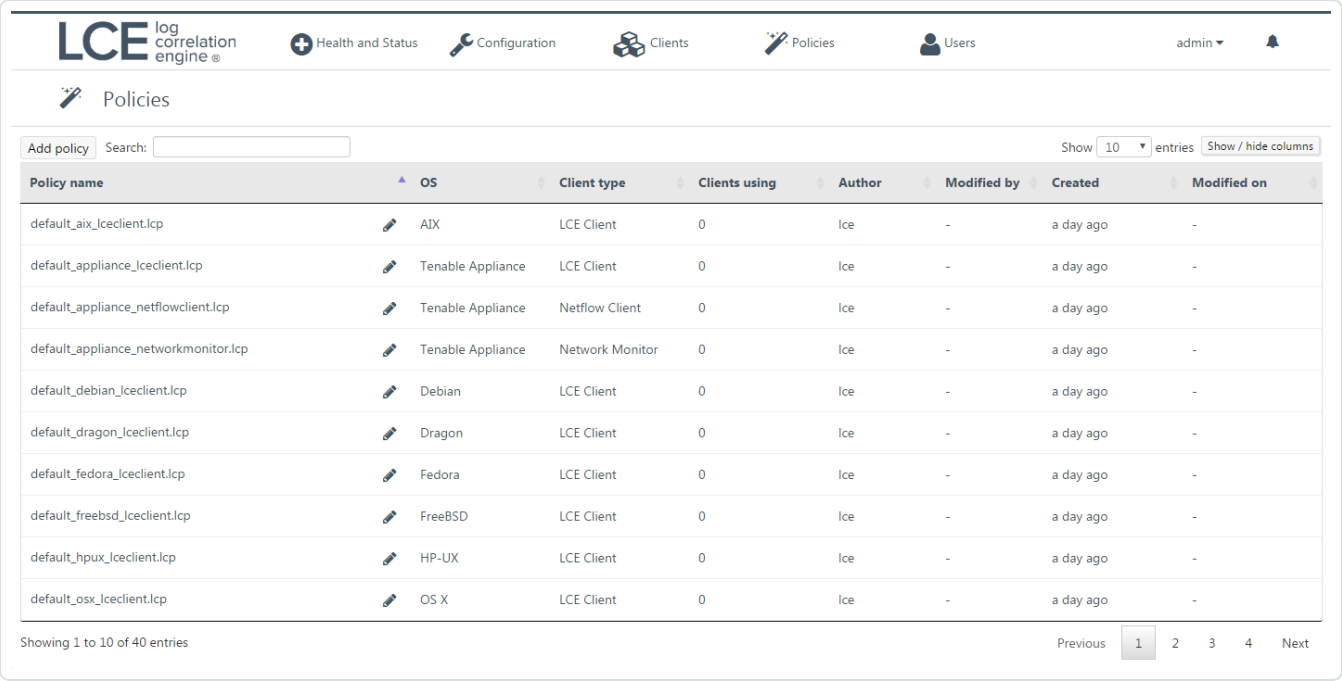
- Create a Client Policy
- Edit an Existing Client Policy
- Clone an Existing Client Policy

Create a Client Policy with the Client Policy Builder

Steps

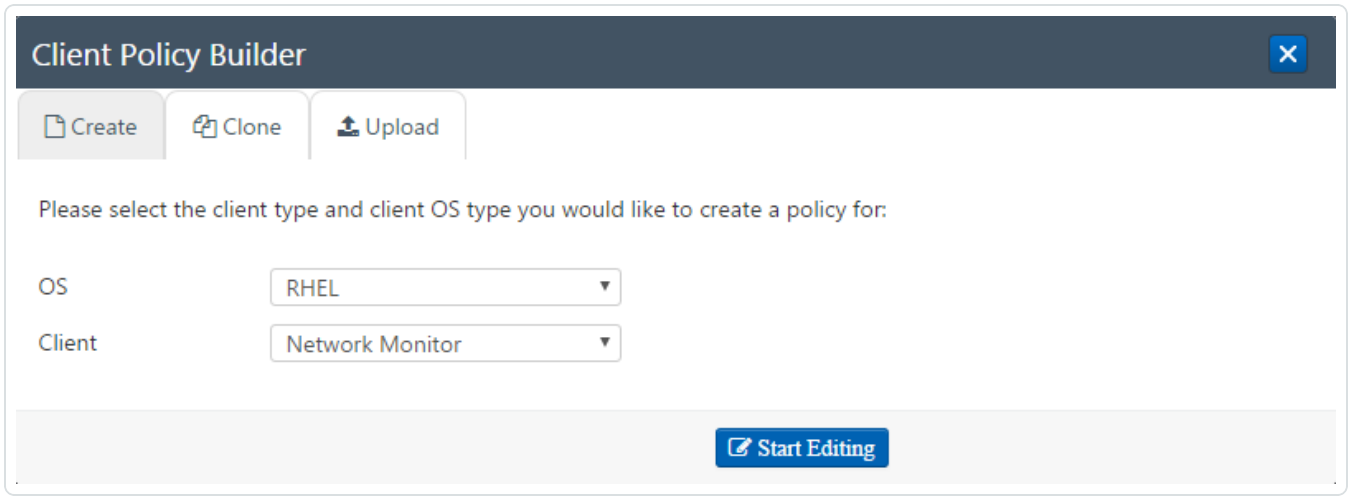
1. In the top navigation bar, click **Policies**.

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



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

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

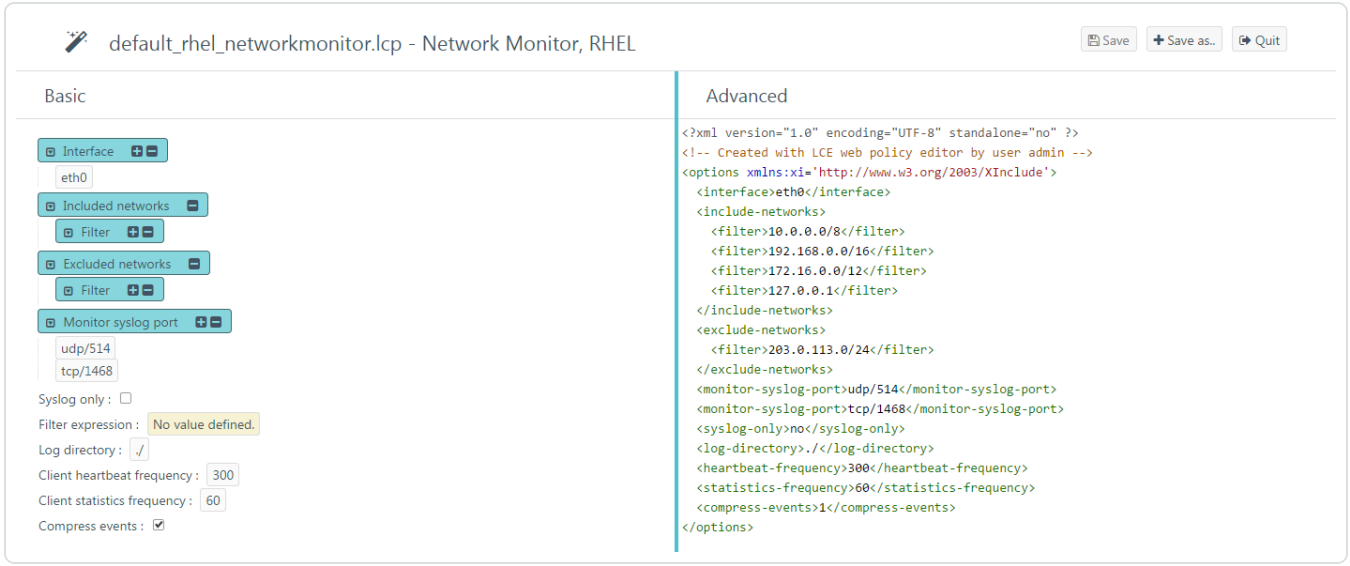


3. In the **OS** list, select the operating system of the host for which you want to create a policy.

   The **Client** list is filtered automatically to display only LCE 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 LCE client for Windows.

4. 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 LCE 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.



> **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.

5. 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., 
   >
   >), 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.

6. Click the **Save as** button.

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

7. 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 LCE 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.

8. Click **OK**.

   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.

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

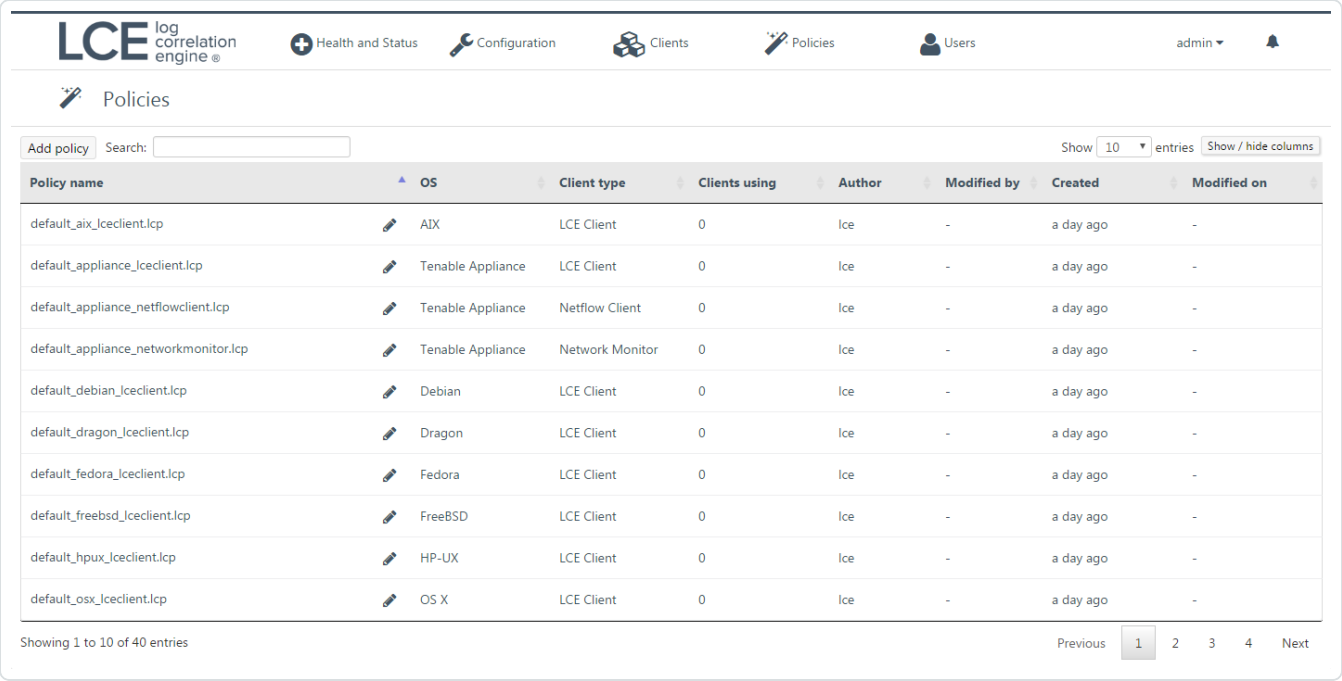
   The **Policies** page appears, displaying a list of default and existing policies.

Edit a Client Policy with the Client Policy Builder

Steps

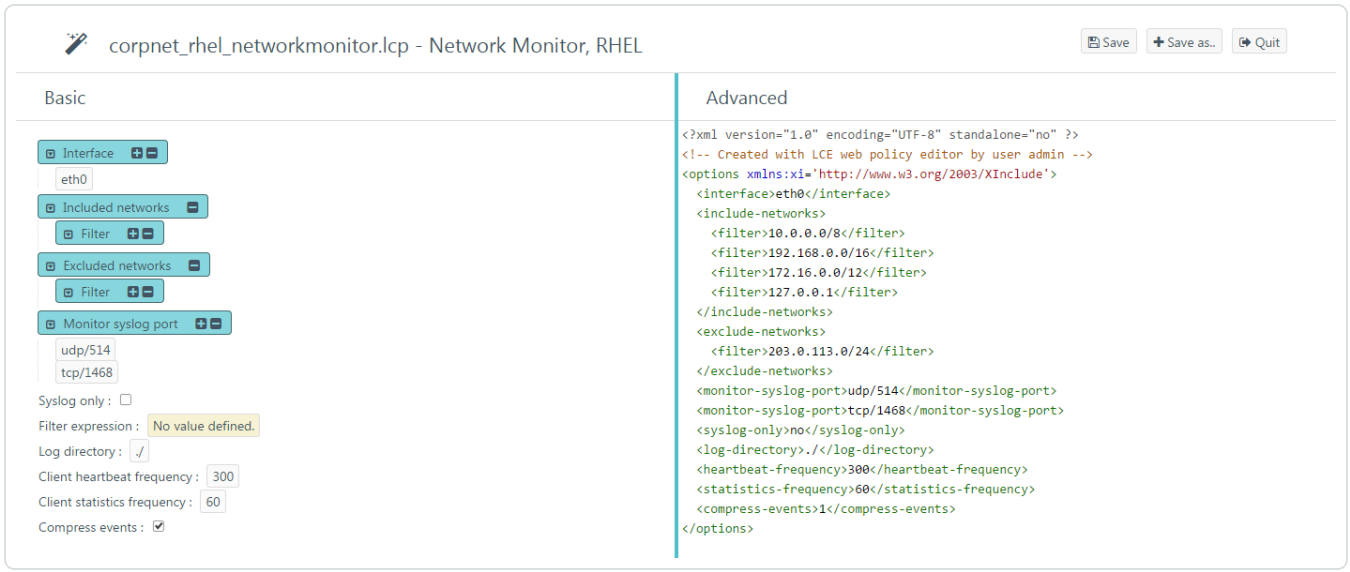
1. In the top navigation bar, click **Policies**.

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



2. 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.

3. 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.

4. 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.

5. 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 LCE 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*.

6. Click **OK**.

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

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

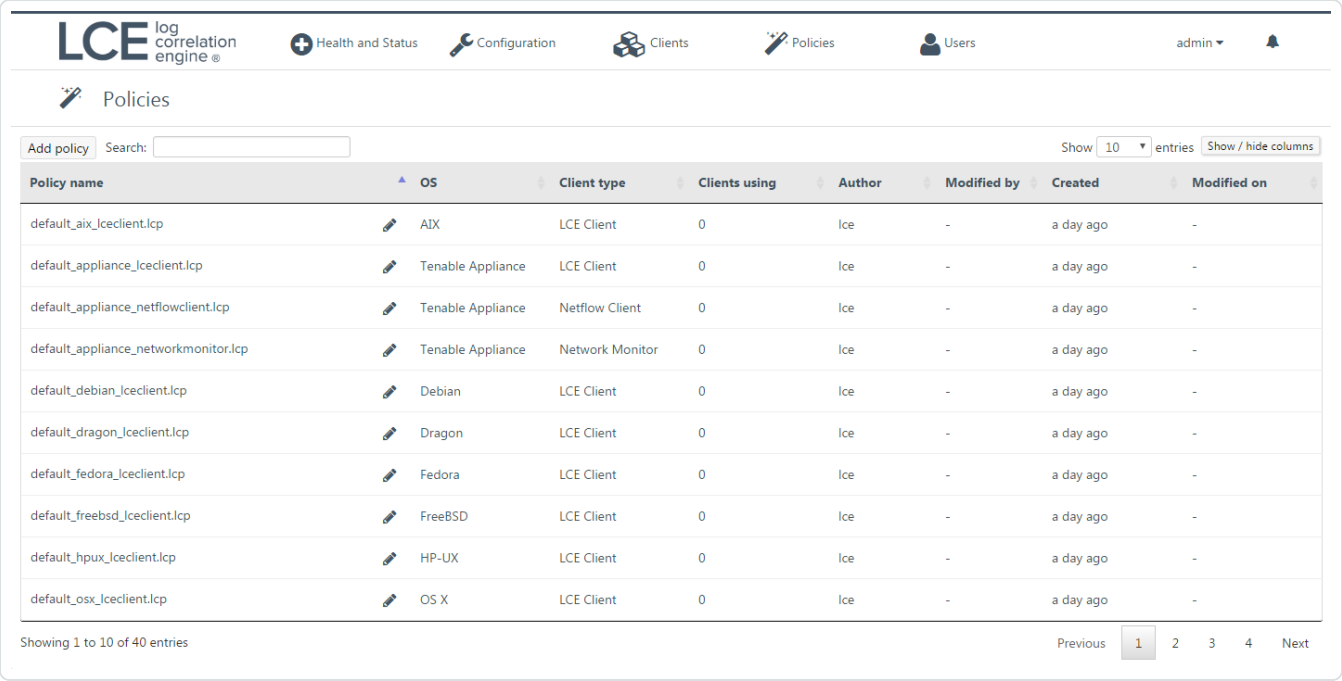
   The **Policies** page appears, displaying a list of default and existing policies. To confirm that the policy you modified was saved, in the upper-right corner of the list of policies, in the **Search** box, type the name of the policy you created, and then check the value in the **Last modified on**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

Clone a Client Policy with the Client Policy Builder

Steps

1. In the top navigation bar, click **Policies**.

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

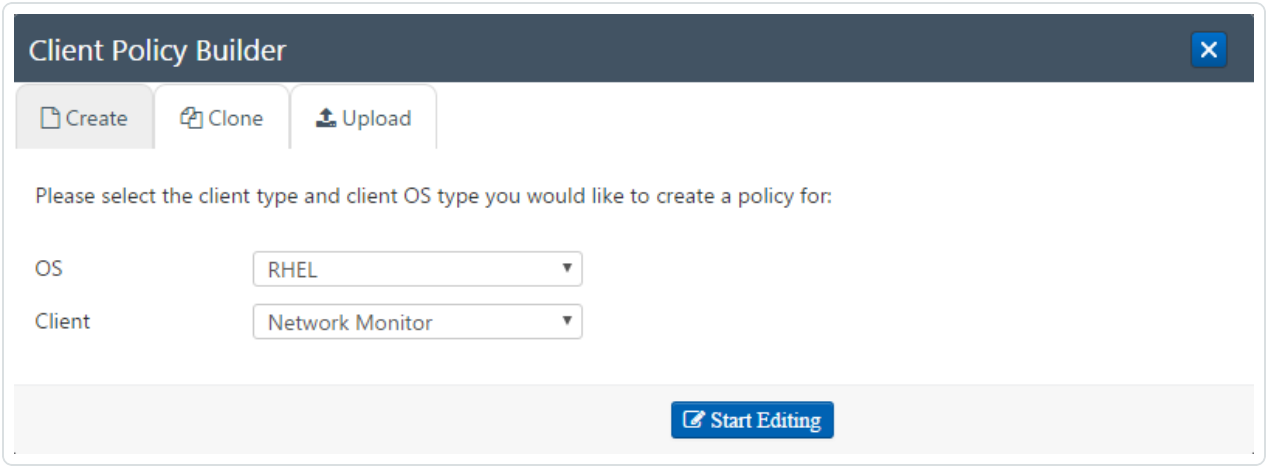


2. In the row corresponding to the policy you want to clone, in the **Actions** column, click the **Clone** button.

   -or-

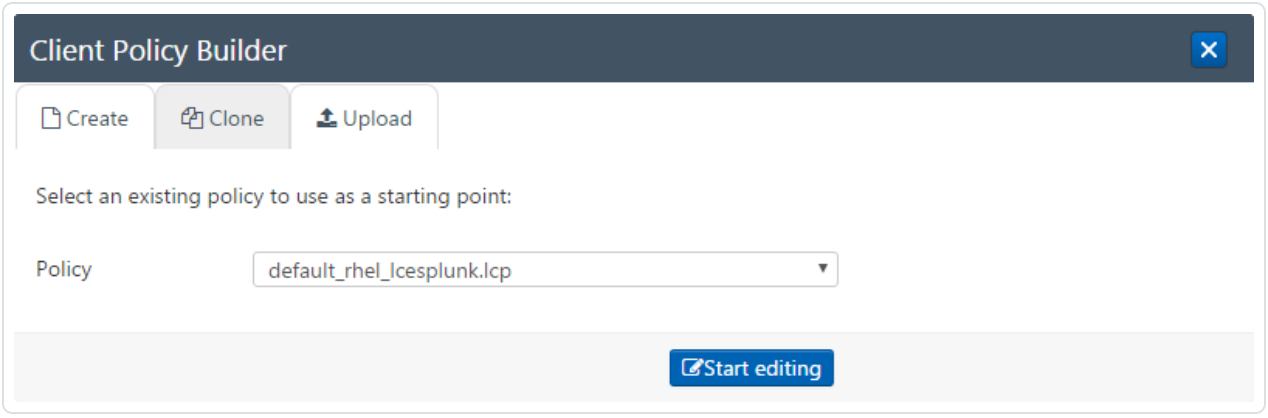
   a. In the upper-left corner of the policy table, click the **Add policy** button.

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



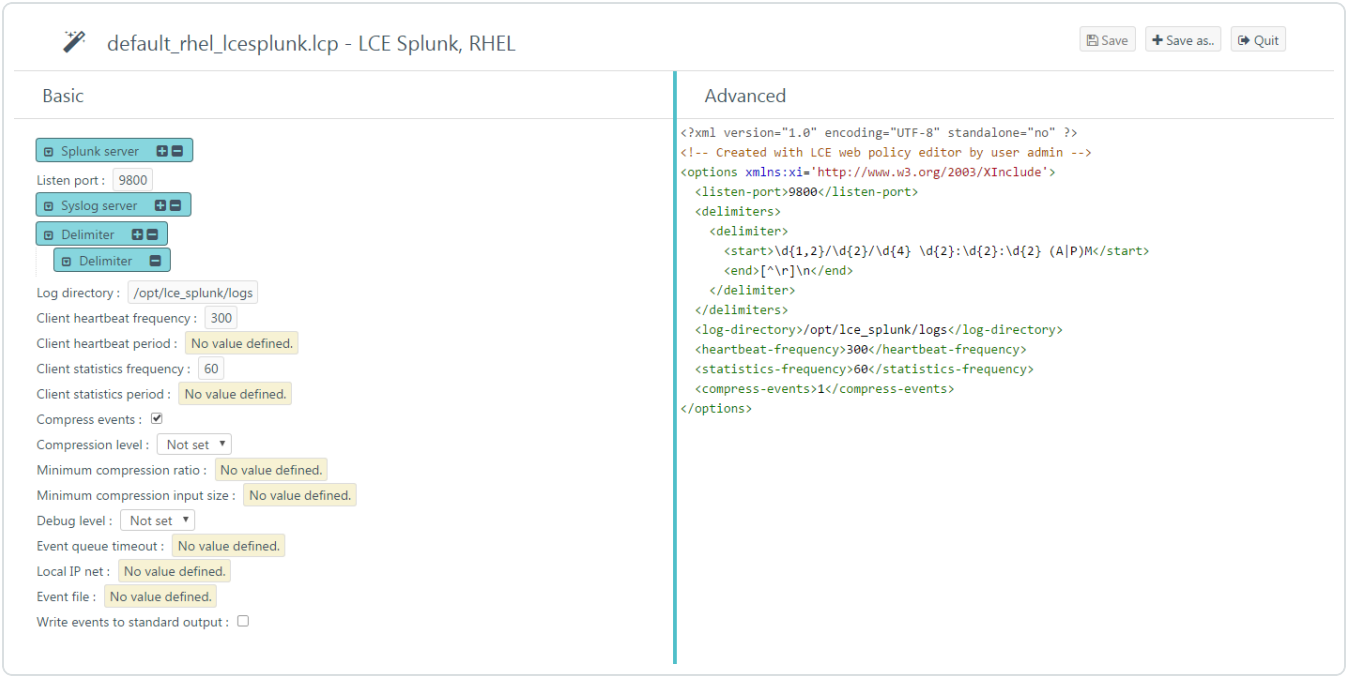
b. Click the **Clone** tab.

The **Clone** section appears.



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.



3. 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.

4. Click the **Save as** button.

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

5. 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 LCE 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*.

6. Click **OK**.

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.

7. 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.

Windows Client Policy Configuration Items

The following table lists the configuration items that are valid for the LCE 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 LCE Windows Client.

Configuration Item	Description	Valid Values

Event log	The name of a Windows event log to monitor. Each event that appears in event logs monitored by the LCE Windows Client are sent to the LCE server individually. You can specify one or more event logs to monitor.
	
	XML Examples:
	
	`<event-log>Microsoft-Windows-Diagnostics-Performance/Operational</event-log>`
	
	`<event-log>all</event-log>`
	
	Tip: To locate event providers that you want to include in your policy, use the Windows Event Viewer.
		The name of the Windows event log (for example, *Application*) that you want to monitor, or the value *all*.
		
		If you specify *all*, in addition to Windows logs, events from Applications and Services logs will also be monitored.

Events to ignore	A provider name that you want the LCE Windows Client to ignore. Additionally, if you do not want to ignore *all* events from a log provider, you can add specific event IDs for that provider.
	
	XML Example:
	
	`<event-log-filter>`
	`  <ignore>`
	`  <provider-name>Microsoft-Windows-Windows`
		The provider name must be a valid log provider.
		
		The event ID must be an integer. It cannot include any letters or sym-

Configuration Item	Description	Valid Values

	<pre>Defender/WHC</provider-name>
	  </ignore>
	  <ignore>
	  <provider-name>Microsoft-Windows-
	TaskScheduler/Operational</provider-name>
	  <event-id>318</event-id>
	  </ignore>
	  <ignore>
	  <provider-name>Microsoft-Windows-
	WindowsUpdateClient/Operational</provider-name>
	  <event-id>41</event-id>
	  <event-id>40</event-id>
	  <event-id>26</event-id>
	  </ignore>
	</event-log-filter></pre>
	Tip: To locate event providers that you want the LCE Windows Client to ignore, use the Windows Event Viewer.
		bols.

Monitor text files	The full path and file name of a text file to monitor. Each new line is sent to LCE as a new log. 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: • Location: The full path that contains text files you want to monitor. Each new line in each file is sent to LCE 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. • Exclude: Files in the folder specified for Location will NOT be monitored if they match the Exclude pattern.	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

	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.
	Caution: If you specify a maximum file size, the LCE 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.
	XML Examples:
	`<flat-file>C:\\Windows\\WindowsUpdate.log</flat-file>`
	`<flat-file><location>C:\\Windows\\</location><include>*.log</include><exclude>iis7.log</exclude><delete-on-size-bytes>4096K</delete-on-size-bytes></flat-file>`	

Monitor binary files	The full path and file name of a non-text file to monitor. If the file changes, the old and new MD5 checksums are sent as an event to the LCE server. The maximum number of files that can be specified is 63. 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 para-	Any fully qualified path and file name, including the file extension. It is best practice to escape folder

Configuration Item	Description	Valid Values

	meters to refine which files are monitored by the client:
	• 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.
	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:
	• Include-dir: Included directory path for monitoring files. Wildcards are allowed.
	• Exclude-dir: Excluded directory path for monitoring files. Wildcards are allowed.
	XML Example:
	`<monitor-file>C:\\Windows\\notepad.exe</monitor-file>`
	`<monitor-file>`
	`<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>`
		separators with a backslash. For example, *C:\\Windows*.

Monitor sub-	Whether to monitor files in subdirectories of the folder spe-	0 (off) or 1 (on)

Configuration Item	Description	Valid Values
directories	cified for Location for Monitor binary files, if those files match the specified pattern. If set to *1*, monitoring an extensive folder structure (such as C:\\Windows) with no include or exclude filters may impact performance. XML Example: `<monitor-subdirectories>1</monitor-subdirectories>`	
Monitor wait seconds	The number of seconds to wait before monitoring files. The default is 5 seconds. XML Example: `<monitor-wait-seconds>10</monitor-wait-seconds>`	An integer greater than 0.
Tail sub-directories	Whether to monitor files in subdirectories of the folder specified for Location for Monitor text files, if those files match the specified pattern. If set to *1*, monitoring an extensive folder structure (such as C:\\Windows) with no include or exclude filters may impact performance. XML Example: `<tail-subdirectories>1</tail-subdirectories>`	0 (off) or 1 (on)
Seconds between scans of logs and text files	The number of seconds between scanning logs monitored by the LCE Windows Client. XML Example: `<interval-log-seconds>30</interval-log-seconds>`	An integer greater than 0.

Configuration Item	Description	Valid Values
Interval monitor	**Caution:** This option is deprecated for the LCE Windows Client versions 4.4 and later.	No valid values
Send new events only	Whether to only send new events. If set to *0*, all data in all monitored logs will be sent to the LCE server every time the client is restarted or when the policy changes. XML Example: `<send-new-events-only>1</send-new-events-only>`	0 (off) or 1 (on)
Monitor config	**Caution:** This option is deprecated for the LCE Windows Client versions 4.4 and later.	No valid values
Report unknown processes	If enabled, the LCE 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. XML Example: `<report-unknown-processes>2</report-unknown-processes>`	0 (off), 1, or 2 • *1*: A list of LCE_Client_Detected_ Unknown_Process events will be sent only once, and subsequently only newly-encountered unknown DLLs and EXEs will

Configuration Item	Description	Valid Values
		be reported. • *2*: The list of reported unknown processes will be cleared every time the client is restarted or a new policy is received. All existing unknown DLLs and EXEs will be sent to the LCE server again.
Remote host to monitor	Using the following parameters, specifies a remote host to monitor: • IP address: The IP address of the host that you want to monitor. • Namespace: The namespace of the WMI classes being monitored, usually *root\cimv2*.	All parameters require values.

Configuration Item	Description	Valid Values

	• 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.
	Note: How are user credentials stored in the policy? Are they encrypted?
	XML Example:
	`<Host>`
	`<ip>172.26.0.10</ip>`
	`<namespace>root\cimv2</namespace>`
	`<domain>?</domain>`
	`<username>corpnetAdmin</username>`
	`<password>argus$12</password>`
	`<logfilename>C:\\Windows\\WindowsUpdate.log</logfilename>`
	`</Host>`	

Info	Enable or disable info-level logging in lce_client.log (the LCE client debugging log). XML Example: `<info>0</info>`	0 (off) or 1 (on)
Verbose	Enable or disable verbose logging in lce_client.log (the LCE client debugging log). XML Example:	0 (off), 1, or 2 • *1*:

Configuration Item	Description	Valid Values
	<verbose>0</verbose>	• *2*: Additional debugging information.
Debug	Whether to enable debugging messages in lce_client.log (the LCE 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. XML Example: <debug>0</debug>	0 (off) or 1 (on)
Client heartbeat frequency	The number of seconds between each client heartbeat message to the LCE server. If set to *0*, the client will not send heartbeats. XML Example: <heartbeat-frequency>600</heartbeat-frequency>	An integer
Client statistics frequency	The number of minutes between each client host performance statistics report (CPU, Disk Space, and Physical Memory) to the LCE server. If set to *0*, client statistics will not be sent. XML Example: <statistics-frequency>60</statistics-frequency>	An integer
Compress events	Whether client will compress log data prior to sending it to the LCE server in order to save bandwidth. Recommended except when debugging. If set to *0*, events will not be compressed.	0 (off) or 1 (on)

Configuration Item	Description	Valid Values
	XML Example: `<compress-events>1</compress-events>`	
Compression level	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. XML Example: `<compression-level>5</compression-level>`	An integer from 1 to 9.
Minimum compression ratio	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 LCE Server decompressing event data when compression benefits are minimal. Ignored unless compression is enabled. XML Example: `<minimum-compression-ratio>1.5</minimum-compression-ratio>`	A decimal number.
Minimum compression input size	The minimum number of bytes a packet must have to be compressed. Ignored unless compression is enabled. XML Example:	An integer greater than 0.

Configuration Item	Description	Valid Values
	<minimum-compression-input-size>2048</minimum-compression-input-size>	
Event queue timeout	Maximum number of seconds between event messages the client sends to the LCE server. XML Example: <event-queue-timeout>30</event-queue-timeout>	An integer greater than 0.
Malware scan period	This option specifies the interval (in seconds) that the LCE Windows Client will scan running processes, and monitored directories. XML Example: <malware-scan-frequency>600</malware-scan-frequency>	An integer greater than 0.
Whitelist hashes	MD5 file hashes that will be ignored by LCE Windows Client that may otherwise be considered malware. XML Example: <whitelist-hashes>8d1ae0900d461fd593b4daf67ee72e00</whitelist-hashes>	An MD5 hash.
Custom malware hashes	MD5 file hashes that will be identified as malware by the LCE Windows Client if detected. XML Example: <custom-malware-hashes>e1112134b6dcc8bed54e0e34d8ac272795e73d74</c-	An MD5 hash.

Configuration Item	Description	Valid Values
	`ustom-malware-hashes>`	