Table of Contents

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.*

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.

How To

Reference

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**.

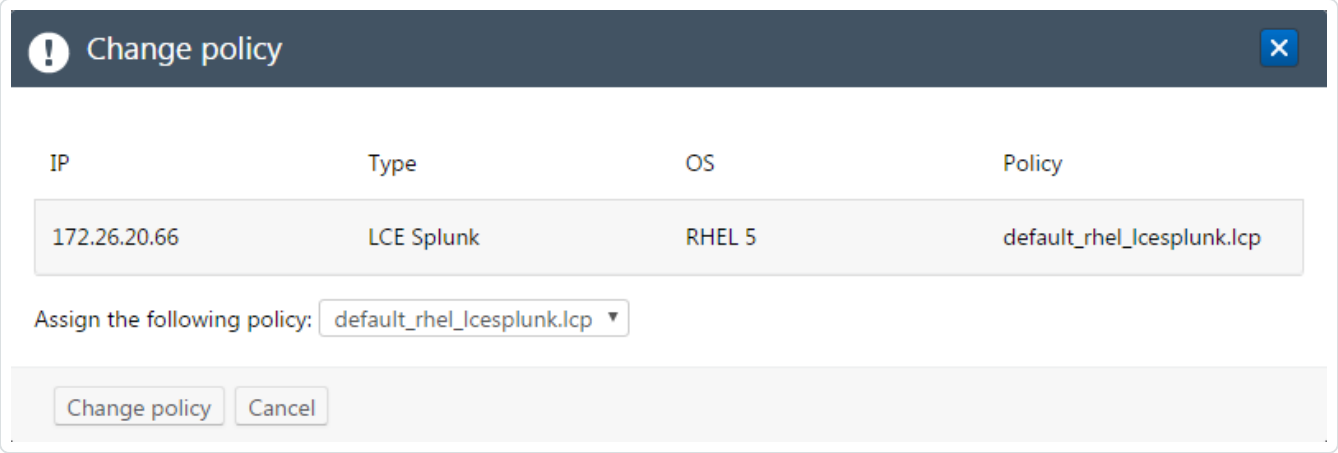
   The **Clients** page appears, displaying the client table.

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.

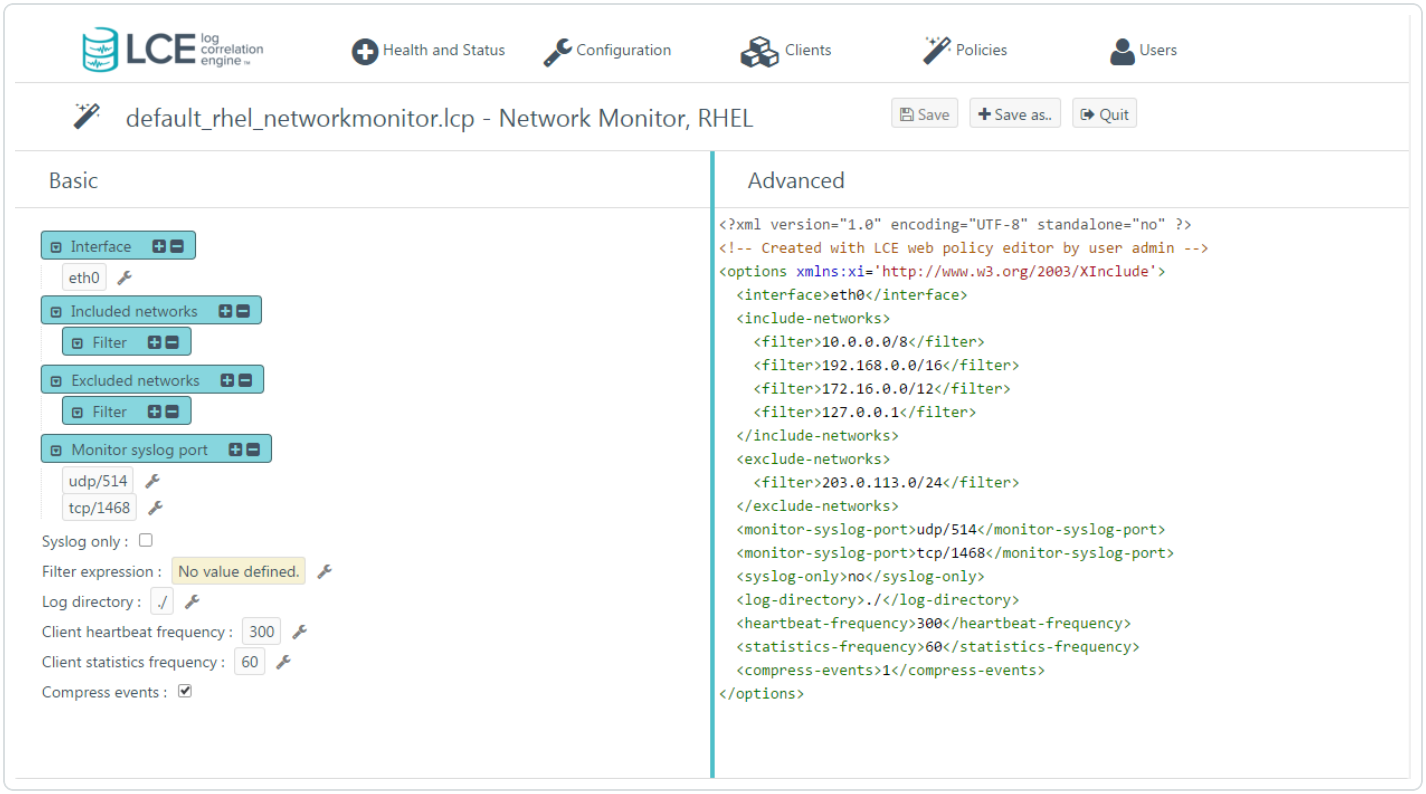


4. In the **Assign the following policy** list, select the policy that you want to assign to the LCE client.
5. Review the LCE client that will have a new policy, and then click the **Change policy** button.

   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:

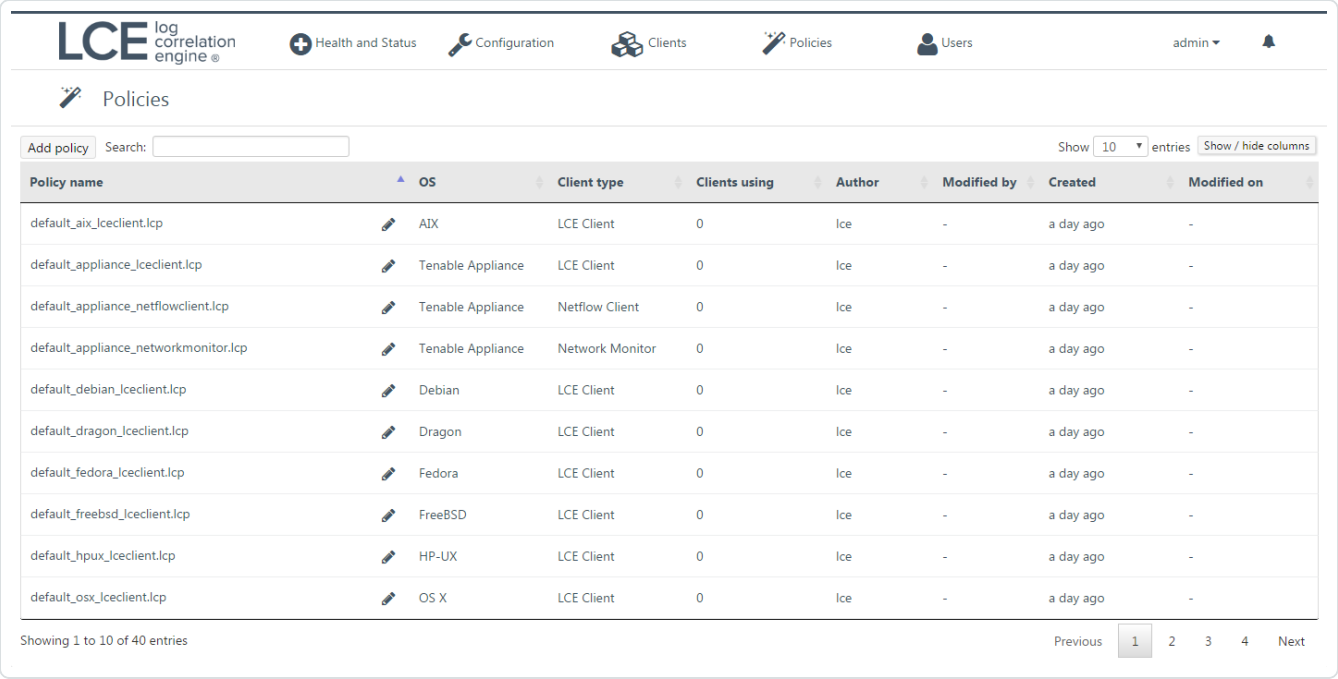
- Create a Client Policy
- Edit an Existing Client Policy
- Clone an Existing Client Policy

Create a Client Policy with the Client Policy Builder

Steps

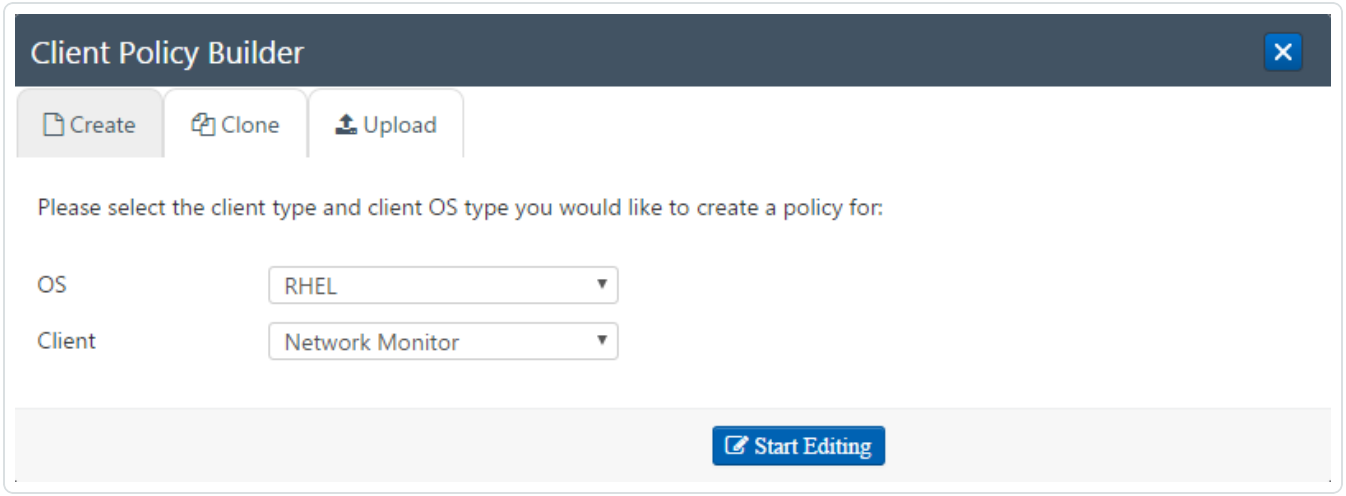
1. In the top navigation bar, click **Policies**.

   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.

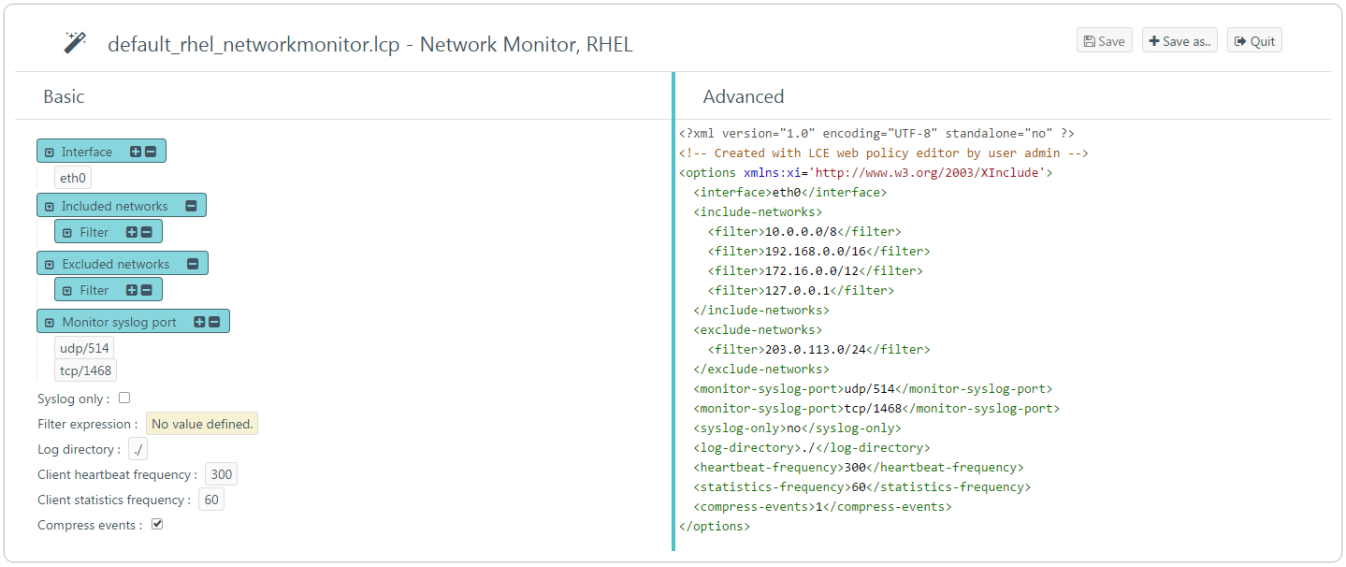


3. In the **OS** list, select the operating system of the host for which you want to create a policy.

   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*.

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.

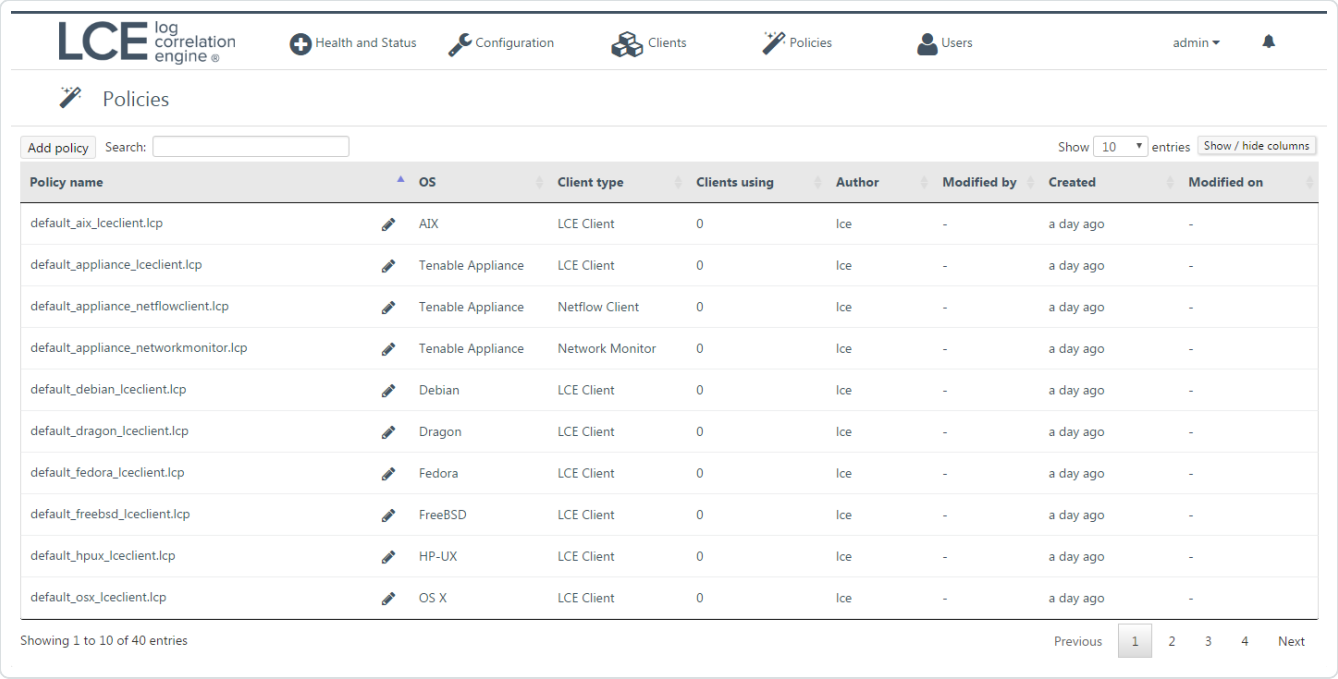
   The **Policies** page appears, displaying a list of default and existing policies.

Edit a Client Policy with the Client Policy Builder

Steps

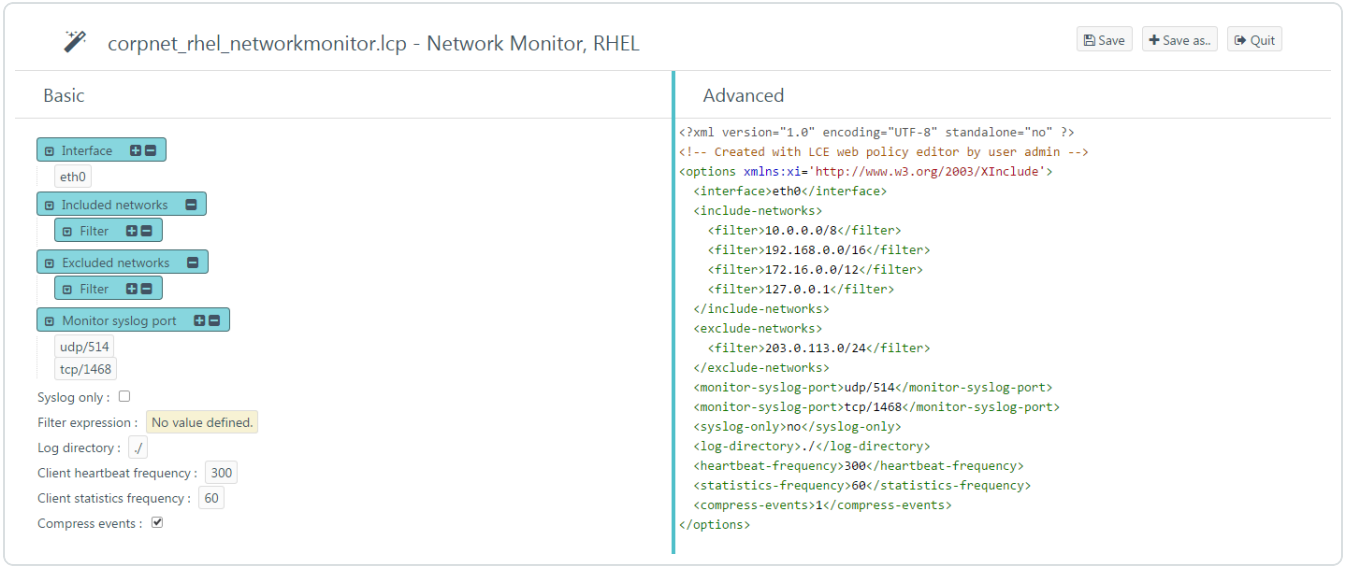
1. In the top navigation bar, click **Policies**.

   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.

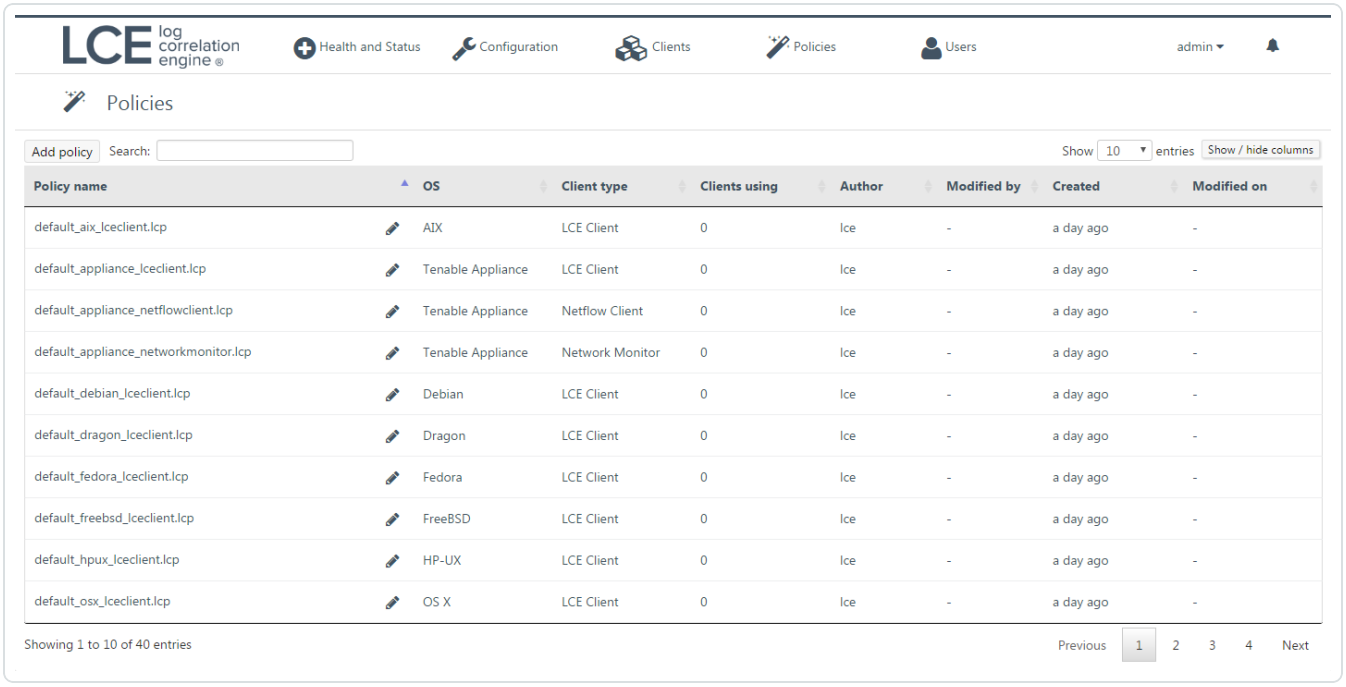
   The **Policies** page appears, displaying a list of default and existing policies. To confirm that the policy you modified was saved, in the upper-right corner of the list of policies, in the **Search** box, type the name of the policy you created, and then check the value in the **Last modified on**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

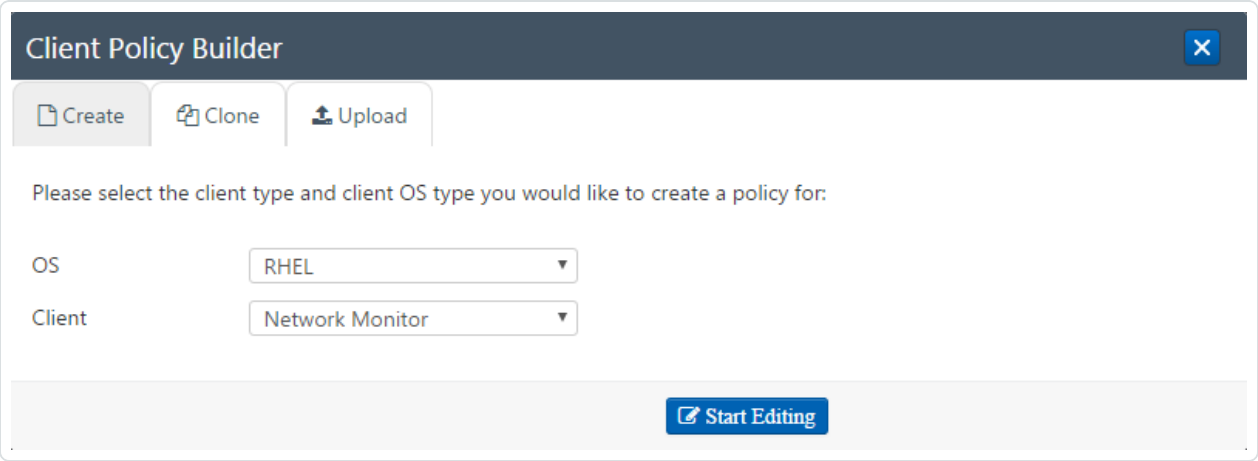


2. In the row corresponding to the policy you want to clone, in the **Actions** column, click the **Clone** button.

   -or-

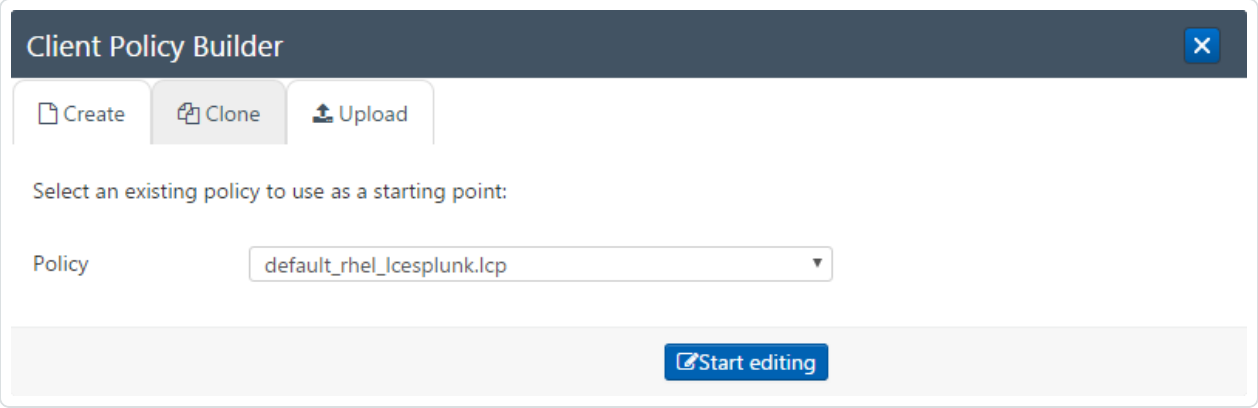
   a. In the upper-left corner of the policy table, click the **Add policy** button.

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



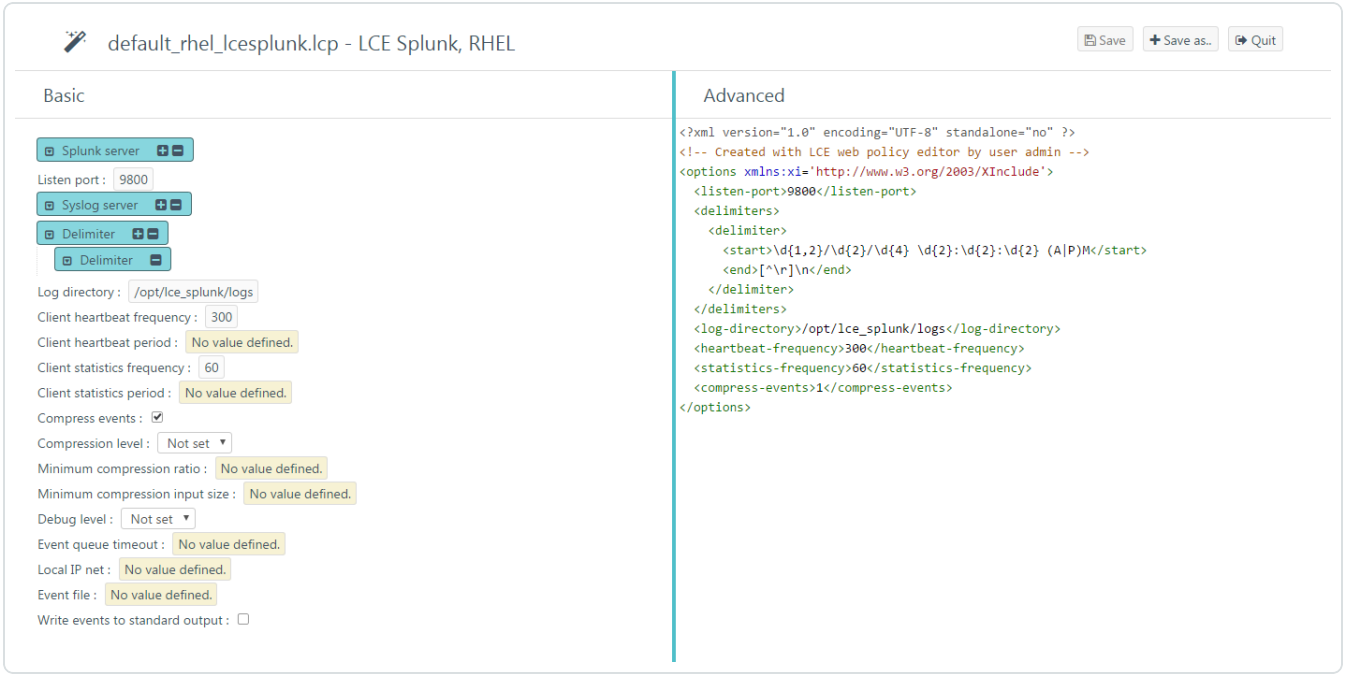
b. Click the **Clone** tab.

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.