



Customer Guide

Creating New Rules in Tripwire Enterprise

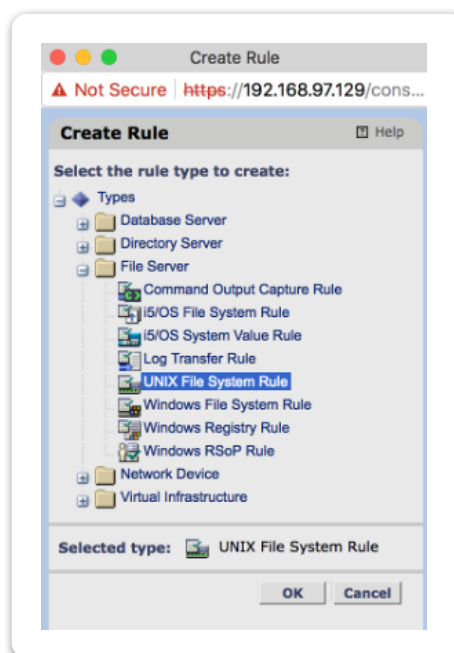
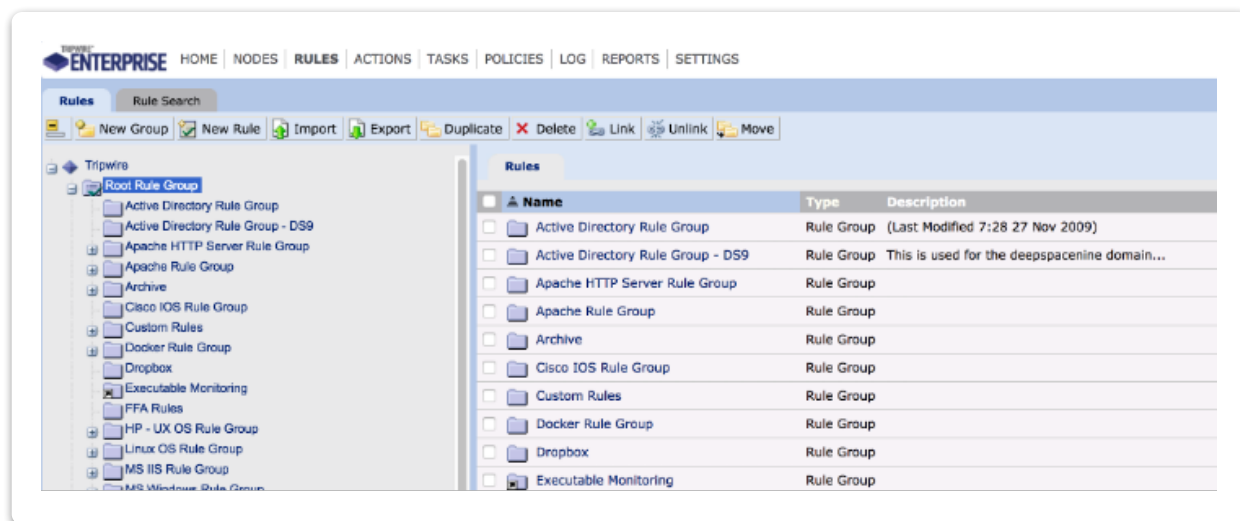


Creating New Rules in Tripwire Enterprise

Each organization is made up of a unique technology ecosystem, so Tripwire enables you to create new rules beyond the default rules and policies within the solution. Part of any deployment of Tripwire® Enterprise is for your organization to decide what objects (files, directories, etc.) are important to monitor and which are not. Use this step-by-step guide to learn how to create new rules in Tripwire Enterprise.

How to create a new rule:

1. Go to the **Rule Manager**
2. In the button bar select **New Rule**. It should be noted that the rule will be created in the location selected in the Navigation tree on the left. If necessary create any new groups needed to logically organize your rule sets.
3. In the **New Rule** dialog box, select the rule type you wish to create. For the purposes of this exercise, select **Windows Rule** or **Unix Rule**.



- On the first page of the new rule wizard provide a name and description of the rule so that other admins or auditors can understand the purpose of the rule. Click **Next**.

The screenshot shows a web browser window titled "New UNIX File System Rule Wizard". The address bar shows a "Not Secure" warning and the URL "https://192.168.97.129/console/app.showWizard.cmd?wizardN...". The main content area has a title bar "New UNIX File System Rule Wizard" with a "Help" icon. Below the title bar, it says "Enter a name and description." There are two input fields: "Name:" with the placeholder text "Name your rule here" and "Description:" with the placeholder text "Its a good idea to document the reason for the rule here in case you get hit by a bus...". Below these fields are two checked checkboxes: "Enable Tracking Identifier" and "Traverse mount points". At the bottom right are four buttons: "< Back", "Next >", "Finish", and "Cancel".

- To create a new specifier (path) in the new rule: If you already know the path to be monitored click either **New Start Point** or **New Stop Point**. If the path is not known...

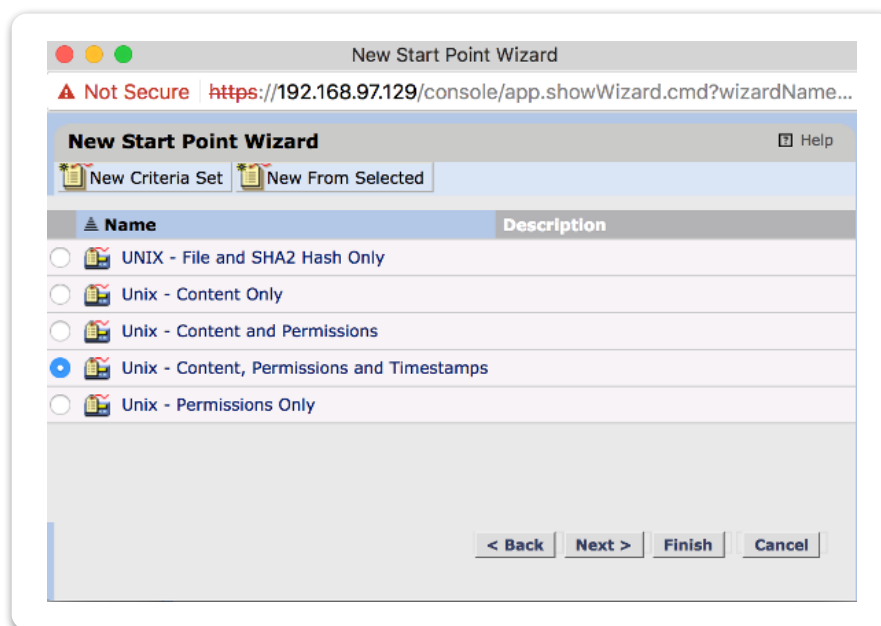
The screenshot shows the same web browser window, now at Step 2. The title bar and address bar are the same. The main content area has a title bar "New UNIX File System Rule Wizard" with a "Help" icon. Below the title bar, there are three buttons: "New Start Point", "New Stop Point", and "Browse", followed by a "Delete" button with a red 'X' icon. Below these buttons is a table with the following headers: "Path", "Type", "Default Severity", "Criteria Set", "Recurse Level", and "Archive Content". The table body is empty. At the bottom right are four buttons: "< Back", "Next >", "Finish", and "Cancel".

6. ...click **Browse**. In the **Select Node** box, drill down to and select a representative node. Once the node is selected you can drill down to the directory or file and click on it. Your choice should be in the **Selected Path** field at the bottom.

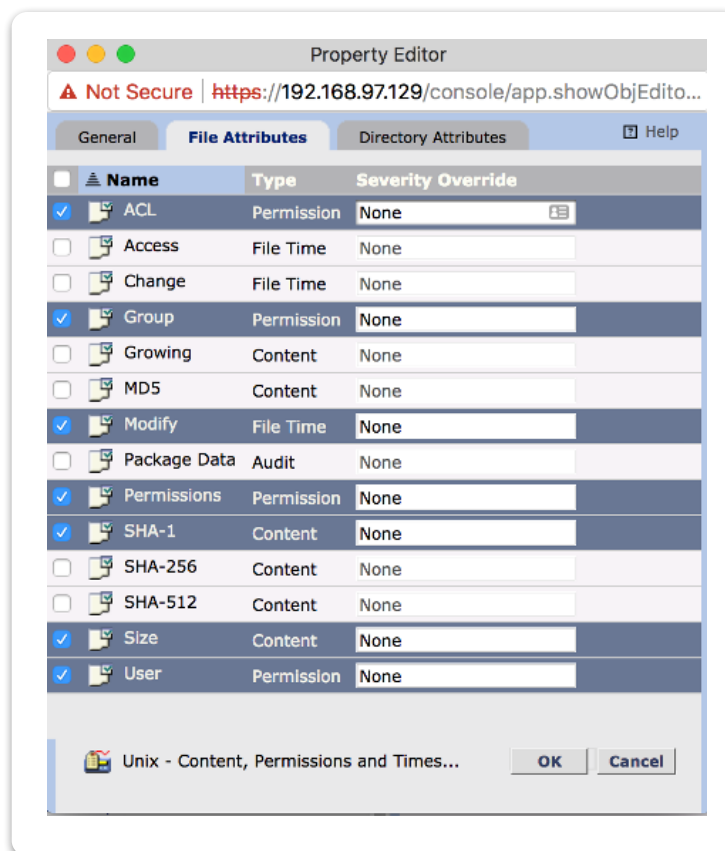


7. Click either **New Start Point** or **New Stop Point**. In the wizard populate the path if it has not already been populated in the previous step.

8. Set your severity level. The default is 10,000 but can be set to any number from 0 to 10,000. Custom severity ranges can be created with different colors to represent in reports or the console.
9. Select **Archive Element Content** if the file or path contains ASCII, HTML or XML files that you want to be able see line-by-line changes.
10. If the path is a directory leave **Recurse Directory** enabled. This will allow the agent to recurse all subdirectories under the root of the selected path. If the path has a lot of subdirectories, it could take a while. You can change the depth in the corresponding field. Click **Next**.
11. Select a **Criteria Set**. This is the list of attributes such as permissions, hashes, time stamps and such. Generally, if the file is not expected to change much you can select one like **Content and Permissions** or **Content, Permissions, and Timestamps**. If the file is known to be dynamic, select **Permissions Only**. Click **Next**.



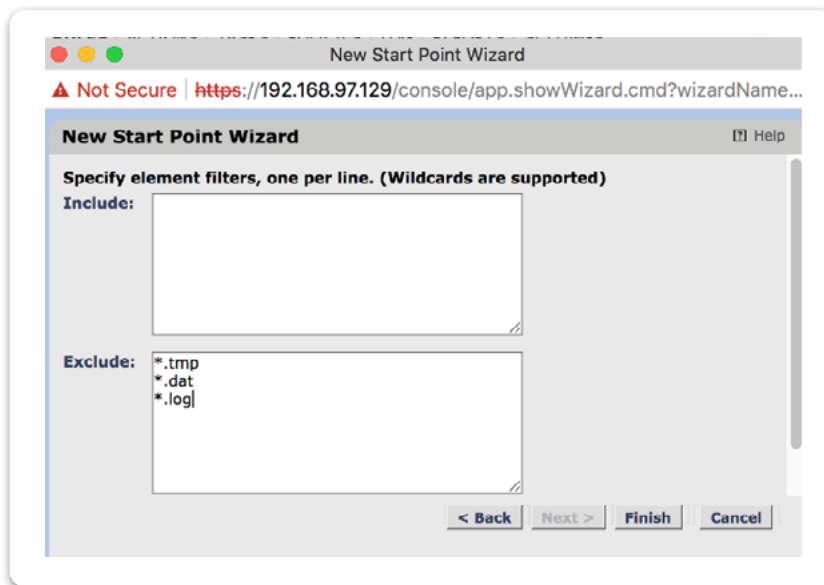
This is what a criteria set looks like if you were to want to edit one. You can enable or disable individual attributes as part of your noise tuning process.



12. If the path is a directory you can choose to filter items. Include is an explicitly set filter. If you enter *.exe in this filter the rule will only monitor files with .exe in the name. The **Exclude** field is Implicit in that if you put *.tmp, all files will be monitored except files with .tmp in the name. Click **Finish**. Repeat this process to create additional specifiers in the rule.

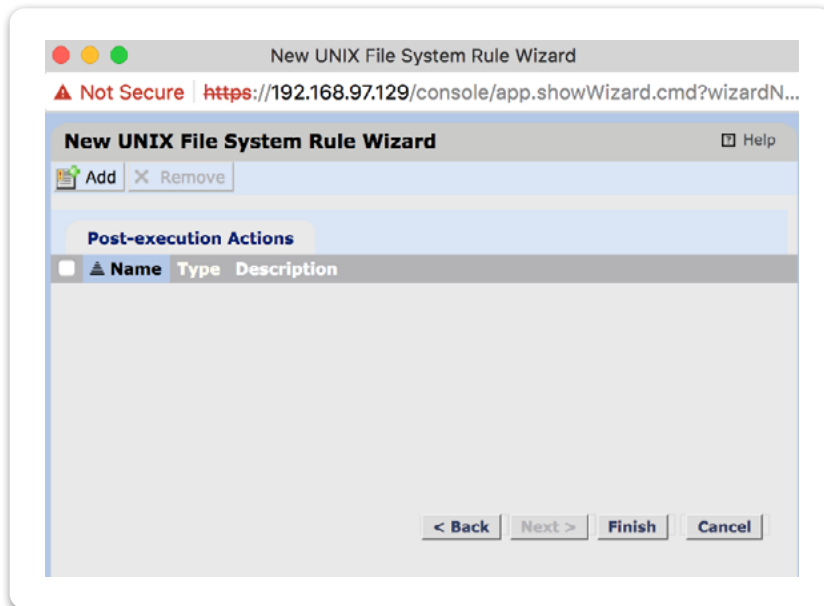
The image displays two sequential screenshots of the 'New Start Point Wizard' dialog box, which is titled 'New Start Point Wizard' and has a 'Help' button in the top right corner. The address bar shows a 'Not Secure' warning and the URL 'https://192.168.97.129/console/app.showWizard.cmd?wizardName...'. The main instruction is 'Specify element filters, one per line. (Wildcards are supported)'. The top screenshot shows the 'Include:' field with the text '*.exe' and '*.dll' entered. The bottom screenshot shows the 'Exclude:' field with the text '*.tmp', '*.dat', and '*.log' entered. Both screenshots have a '< Back' button, a 'Next >' button, a 'Finish' button, and a 'Cancel' button at the bottom right.

13. When done creating specifiers click **Next**. Enable real-time monitoring if you want to monitor these paths with the Tripwire Event Generator. (Note: Collect audit event information and real-time monitoring must be enabled on the node as well.) Click **Finish**. The new rule is now built.



The screenshot shows a web browser window with the title "New Start Point Wizard". The address bar shows a "Not Secure" warning and the URL "https://192.168.97.129/console/app.showWizard.cmd?wizardName...". The main content area is titled "New Start Point Wizard" and includes a "Help" icon. Below the title, it says "Specify element filters, one per line. (Wildcards are supported)". There are two text input fields: "Include:" which is empty, and "Exclude:" which contains the text "*.tmp", "*.dat", and "*.log". At the bottom right, there are four buttons: "< Back", "Next >", "Finish", and "Cancel".

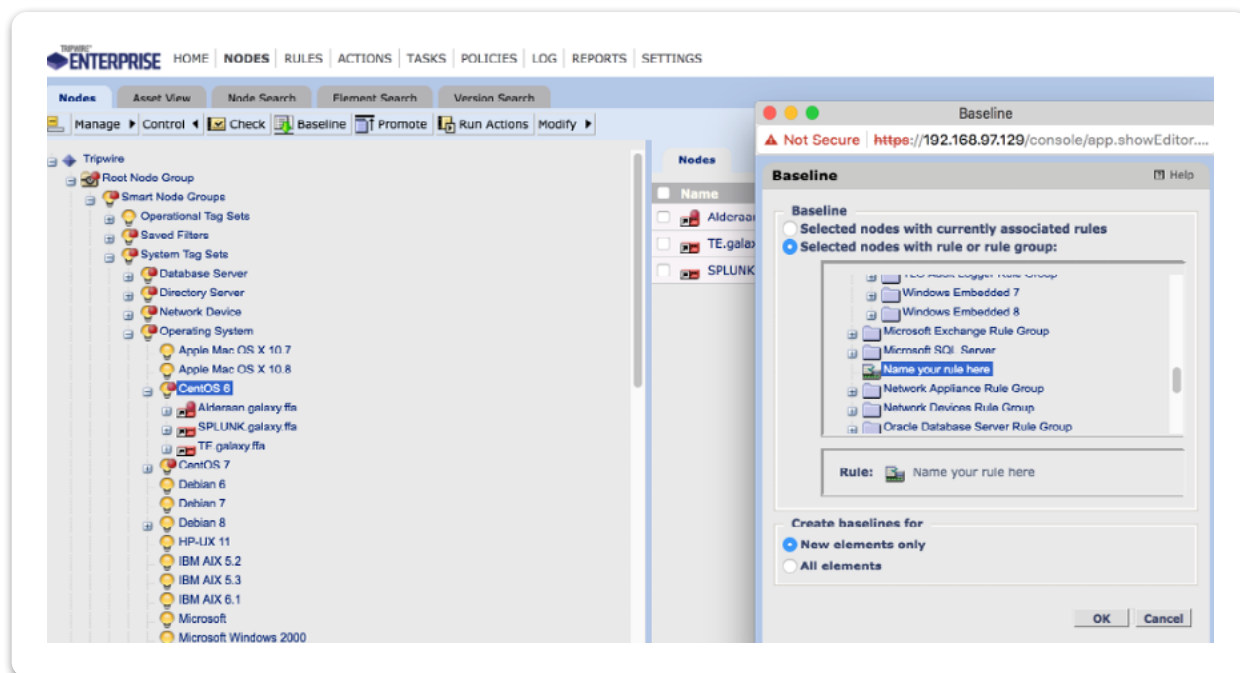
14. Enabling an action on a rule is optional. If you enable real-time monitoring, you will want to add one here because the rule probably won't be part of a separate task which is where actions are typically assigned.



The screenshot shows a web browser window with the title "New UNIX File System Rule Wizard". The address bar shows a "Not Secure" warning and the URL "https://192.168.97.129/console/app.showWizard.cmd?wizardN...". The main content area is titled "New UNIX File System Rule Wizard" and includes a "Help" icon. Below the title, there are "Add" and "Remove" buttons. A section titled "Post-execution Actions" is visible, containing a table with columns "Name", "Type", and "Description". The table is currently empty. At the bottom right, there are four buttons: "< Back", "Next >", "Finish", and "Cancel".

15. After building the rule, you can either create a new task to schedule the integrity check of the new rule and create the baseline. Or if you enabled real-time monitoring, you can manually baseline a node or group of nodes from the **Nodes Manager**.

Only select **All Elements** if you need to re-baseline a node because you messed something up and want to start over again. Otherwise, as you add new nodes to a group as long as **New Elements** only is selected, any existing nodes with baselines with the same rule will not be affected by the baseline. Let the new rule run for a few days, watch the data that is generated—and if necessary, fine-tune the rule to eliminate noise.



Visit the Forums in the Tripwire Customer Center

We hope this guide was helpful in your efforts to get the most out of Tripwire Enterprise. If you have any further questions, the Tripwire forums are the best place for customers to ask technical questions, learn new Tripwire skills, and connect with Tripwire and its customer community about product and feature improvements. Over 200 internal Tripwire experts and employees are ready to answer your questions.

Subscribe to your relevant forum channels to receive alerts about important product issues that may affect your environment. You can customize your preferences around alerts for Tripwire Enterprise, Tripwire IP360™, Tripwire Axon®, and other Tripwire solutions.

Take a moment to explore the [Tripwire Forums](#) and get involved.



Tripwire is the trusted leader for establishing a strong cybersecurity foundation. We protect the world's leading organizations against the most damaging cyberattacks, keeping pace with rapidly changing tech complexities to defend against ever-evolving threats for more than 20 years. On-site and in the cloud, our diverse portfolio of solutions find, monitor and mitigate risks to organizations' digital infrastructure—all without disrupting day-to-day operations or productivity. Think of us as the invisible line that keeps systems safe. **Learn more at tripwire.com**

The State of Security: News, trends and insights at tripwire.com/blog
Connect with us on [LinkedIn](#), [Twitter](#) and [Facebook](#)

©2022 Tripwire, Inc. Tripwire, LogCenter, IP360, Tripwire Axon and others are trademarks or registered trademarks of Tripwire, Inc. All other product and company names are property of their respective owners. All rights reserved.

BRTECNRCG1a 2203