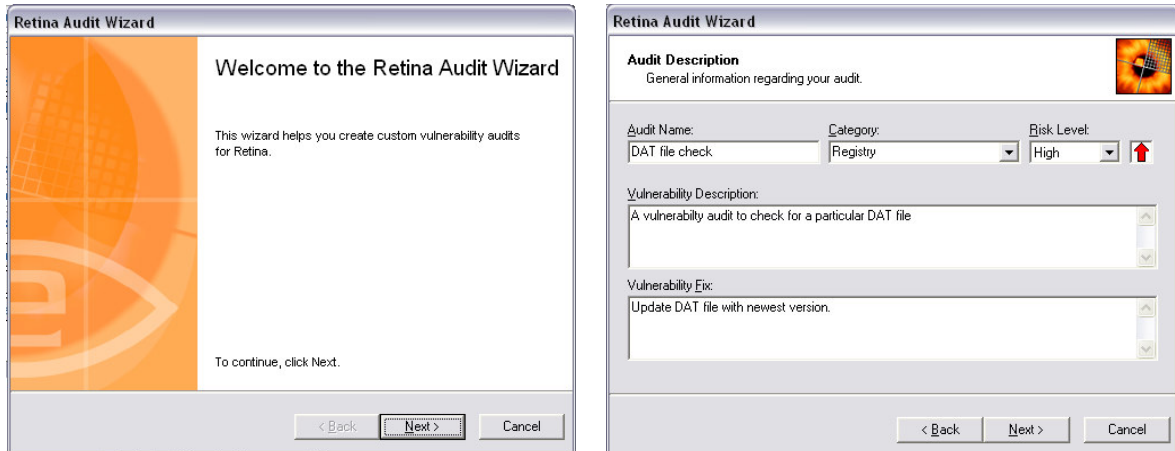


## Creating a Custom Audit in Retina® 5.0

Using the Retina® Audit Wizard, custom audits can be created to help enforce internal policies and standards, such as application version control, monitoring non-approved application usage and enforcing configuration standards.

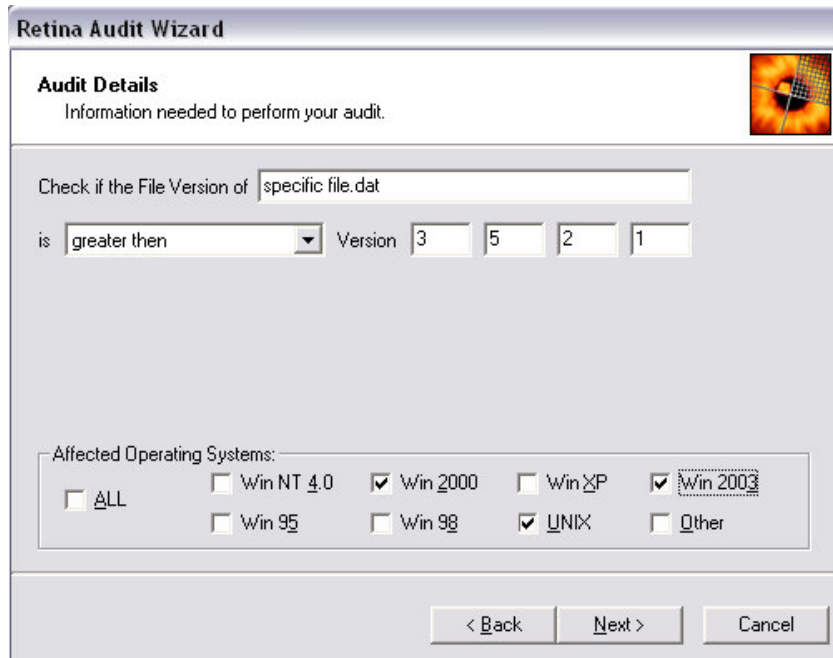
In the example demonstrated below, we are creating a custom audit to check for the presence and version number of a particular DAT file. To begin, from the Retina interface, select Tools → Audits Wizard.



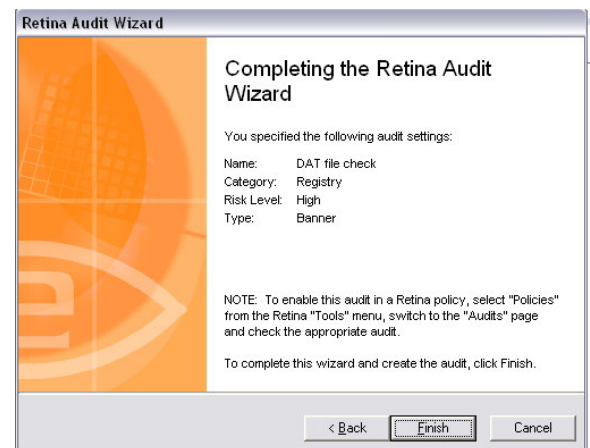
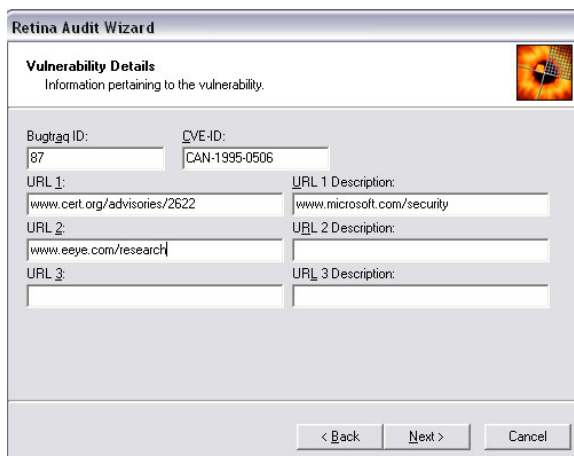
As shown in the examples above, the first step in the Retina Audit Wizard allows us to name the audit and assign it a risk level that will enumerate the criticality of the vulnerability within the network. Vulnerability and fix descriptions can also be added as needed.



There are multiple types of audits that can be created within Retina, and as a result of its open architecture, more can be added according to your needs. This example shows the creation of an audit to 'Check File Version' to assist with the enforcement of versioning control. As you can see, registry key, CGI script and service pack/hotfix audits can also be created.



The next step of the Audit Wizard allows users to specify which file is to be located and the detailed version number that is to be enforced, as well as which platforms on which to search for this file.



Lastly, we can add any Bugtraq, CVE or URL information, perhaps where a new DAT file can be found and downloaded.

This audit will now appear in the Audit Groups pane as a single audit option. For instructions on how to create additional audits, please contact [support@eeye.com](mailto:support@eeye.com).