TOC

Windows Auditing Reference

This interactive spreadsheet helps you configure the audit policy in your environment for successful gathering and real-time monitoring in InTrust.

For gathering, the set of events to be audited is defined by the reports you plan to use. For real-time monitoring, the selection of audited events depends on the rules you are going to deploy.

Event Filter for Gathering and Reporting

To get information about what audit policies should be enabled to view specific reports, or what events a particular report displays, use the **Select** tab.

When you click **Display Result** in the **Select** tab, you are taken to the **Result** tab, which lists the events used in the selected reports. Windows versions prior to Vista have different event IDs /than the corresponding events in Vista and later. Note that the **Result** tab does not show which events correspond to which in the different Windows versions. It just shows which events you need.

Using Reference Tables

Table rows in the **Gathering and Real-Time Monitoring** worksheets show dependencies among the events you need to audit, audit policies you need to have enabled, InTrust policies that must be turned on, reports that require such settings and so on. Use the list boxes with column titles on them to select items that you are interested in. This narrows the scope of table contents for easy reference. To display the entire table again, select **All** in each list box.

Use the **Download this document** link above to download the **InTrust_11.6.1_WindowsAuditingReferences.xls** spreadsheet.