

Windows AppLocker

Windows AppLocker allows administrators to create rules restricting which executables, scripts, and other files users are allowed to run. For more information, see What Is AppLocker? on Microsoft Docs.

AppLocker logs events to the Windows Event Log. There are four logs available, shown in the Event Viewer under **Applications and Services Logs > Microsoft > Windows > Applocker**:

- EXE and DLL
- MSI and Script
- Packaged app-Deployment
- Packaged app-Execution

NXLog can collect these events with the im_msvistalog module or other Windows Event Log modules.

Example 1. Collecting AppLocker logs from Windows Event Log

The following configuration uses the im_msvistalog module to collect AppLocker events from the four Windows Event Log channel sources listed above. The *xm_xml* parse_xml() procedure is used to further parse the **UserData** XML portion of the event.

() This website uses cookies

NAC and a spirit to be represented as a spirit when the spirit and the spirit and

we use cookies to personalise content and aas, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners.

OK

```
<QueryXML>
          <QueryList>
              <Query Id="0">
                  <Select Path="Microsoft-Windows-AppLocker/MSI and Scrip</pre>
                      *</Select>
                  <Select Path="Microsoft-Windows-AppLocker/EXE and DLL">
                      *</Select>
                  <Select Path="Microsoft-Windows-AppLocker/Packaged app-</pre>
                      *</Select>
                  <Select Path="Microsoft-Windows-AppLocker/Packaged app-</pre>
                      *</Select>
              </Query>
          </QueryList>
     </QueryXML>
              if $UserData parse_xml($UserData);
     Exec
 </Input>
Output Sample
   "EventTime": "2019-01-09T22:34:44.164099+01:00",
   "Hostname": "Host.DOMAIN.local",
   "Keywords": "9223372036854775808",
   "EventType": "ERROR",
   "SeverityValue": 4,
   "Severity": "ERROR",
   "EventID": 8004,
   "SourceName": "Microsoft-Windows-AppLocker",
   "ProviderGuid": "{CBDA4DBF-8D5D-4F69-9578-BE14AA540D22}",
   "Version": 0,
   "TaskValue": 0,
   "OpcodeValue": 0.
   "RecordNumber" · 40
```

This website uses cookies

we use cookies to personalise content and aas, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners.

OK

```
"Upcode": "Into",
  "UserData": "<RuleAndFileData xmlns='http://schemas.microsoft.com/sch
  "EventReceivedTime": "2019-01-09T22:34:45.773240+01:00",
  "SourceModuleName": "in".
  "SourceModuleType": "im_msvistalog",
  "RuleAndFileData.PolicyNameLength": "3",
  "RuleAndFileData.PolicyName": "EXE",
  "RuleAndFileData.RuleId": "{4C8E638D-3DE8-4DCB-B0E4-B0597074D06B}",
  "RuleAndFileData.RuleNameLength": "113",
  "RuleAndFileData.RuleName": "WORDPAD.EXE, in MICROSOFT® WINDOWS® OPER
  "RuleAndFileData.RuleSddlLength": "179",
  "RuleAndFileData.RuleSddl": "D:(XD;;FX;;;S-1-1-0;((Exists APPID://FQB
  "RuleAndFileData.TargetUser": "S-1-5-21-314323950-2314161084-42346909
  "RuleAndFileData.TargetProcessId": "7964",
  "RuleAndFileData.FilePathLength": "49",
  "RuleAndFileData.FilePath": "%PROGRAMFILES%\\WINDOWS NT\\ACCESSORIES\
  "RuleAndFileData.FileHashLength": "0",
  "RuleAndFileData.FgbnLength": "118",
  "RuleAndFileData.Fqbn": "O=MICROSOFT CORPORATION, L=REDMOND, S=WASHIN
}
```

Disclaimer

While we endeavor to keep the information in this topic up to date and correct, NXLog makes no representations or warranties of any kind, express or implied about the completeness, accuracy, reliability, suitability, or availability of the content represented here. We update our screenshots and instructions on a best-effort basis.

Last revision: 23 February 2019

Did you like this article?





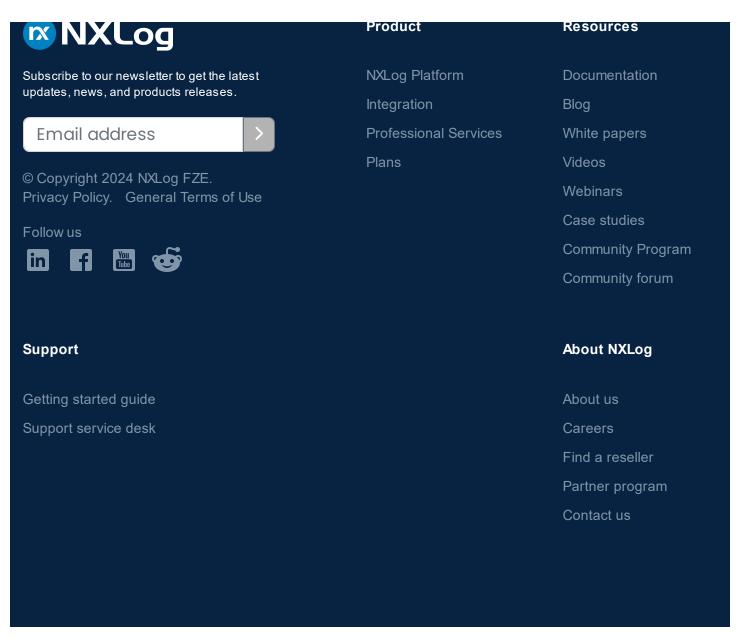
Please leave review about it



(:) This website uses cookies

we use cookies to personalise content and aas, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners.





This website uses cookies