|  |
| --- |
| The MITRE Corporation |
| The OVAL® Language Windows Component Model Specification |
| Version 5.11 |
|  |
| **Danny Haynes, Stelios Melachrinoudis** |
| **2/20/2013** |

|  |
| --- |
| The Open Vulnerability and Assessment Language (OVAL®) is an international, information security, community standard to promote open and publicly available security content, and to standardize the transfer of this information across the entire spectrum of security tools and services. By standardizing the three main steps of the assessment process: representing configuration information of systems for testing; analyzing the system for the presence of the specified machine state; and reporting the results of the assessment, the OVAL Language provides a common and structured format that facilitates collaboration and information sharing among the information security community as well as interoperability among tools. This document defines the Microsoft Windows platform-specific data model for the OVAL Language. |

# Acknowledgements

# Trademark Information

OVAL and the OVAL logo are registered trademarks of The MITRE Corporation. All other trademarks are the property of their respective owners.

# Warnings

MITRE PROVIDES OVAL "AS IS" AND MAKES NO WARRANTY, EXPRESS OR IMPLIED, AS TO THE ACCURACY, CAPABILITY, EFFICIENCY, MERCHANTABILITY, OR FUNCTIONING OF OVAL. IN NO EVENT WILL MITRE BE LIABLE FOR ANY GENERAL, CONSEQUENTIAL, INDIRECT, INCIDENTAL, EXEMPLARY, OR SPECIAL DAMAGES, RELATED TO OVAL OR ANY DERIVATIVE THEREOF, WHETHER SUCH CLAIM IS BASED ON WARRANTY, CONTRACT, OR TORT, EVEN IF MITRE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES[[1]](#footnote-1).

# Feedback

The MITRE Corporation welcomes any feedback regarding the OVAL Language Windows Component Model Specification. Please send any comments, questions, or suggestions to the public OVAL Developer's Forum at [oval-developer-list@lists.mitre.org](mailto:oval-developer-list@lists.mitre.org) or directly to the OVAL Moderator at [oval@mitre.org](mailto:oval@mitre.org)[[2]](#footnote-2).

Contents

[Acknowledgements 1](#_Toc314685995)

[Trademark Information 1](#_Toc314685996)

[Warnings 1](#_Toc314685997)

[Feedback 1](#_Toc314685998)

[1. Introduction 6](#_Toc314685999)

[1.1 Document Conventions 6](#_Toc314686000)

[1.2 Document Structure 7](#_Toc314686001)

[2. OVAL Language Windows Component Model 8](#_Toc314686002)

[2.1 Data Model Conventions 8](#_Toc314686003)

[2.2 win-def:file\_test 8](#_Toc314686004)

[2.2.1 Known Supported Platforms 8](#_Toc314686005)

[2.3 win-def:file\_object 9](#_Toc314686006)

[2.4 win-def:FileBehaviors 11](#_Toc314686007)

[2.5 win-def:file\_state 12](#_Toc314686008)

[2.6 win-sc:file\_item 19](#_Toc314686009)

[2.7 win-def:EntityStateFileTypeType 27](#_Toc314686010)

[2.8 win-sc:EntityItemFileTypeType 27](#_Toc314686011)

[2.12. win-def:EntityStateWindowsViewType 27](#_Toc314686012)

[2.13. win-sc:EntityItemWindowsViewType 28](#_Toc314686013)

[2.14. win-def:registry\_test 28](#_Toc314686014)

[2.14.1. Known Supported Platforms 29](#_Toc314686015)

[2.15. win-def:registry\_object 29](#_Toc314686016)

[2.16. win-def:RegistryBehaviors 31](#_Toc314686017)

[2.17. win-def:registry\_state 33](#_Toc314686018)

[2.18. win-sc:registry\_item 36](#_Toc314686019)

[2.19. win-def:EntityObjectRegistryHiveType 39](#_Toc314686020)

[2.20. win-def:EntityStateRegistryHiveType 40](#_Toc314686021)

[2.21. win-sc:EntityItemRegistryHiveType 40](#_Toc314686022)

[2.22. win-def:EntityStateRegistryTypeType 40](#_Toc314686023)

[2.23. win-sc:EntityItemRegistryTypeType 41](#_Toc314686024)

[2.24. win-def:fileeffectiverights53\_test 42](#_Toc314686025)

[2.24.1. Known Supported Platforms 42](#_Toc314686026)

[2.25. win-def:fileeffectiverights53\_object 42](#_Toc314686027)

[2.26. FileEffectiveRights53Behaviors 45](#_Toc314686028)

[2.27. win-def:fileeffectiverights53\_state 47](#_Toc314686029)

[2.28. win-sc:fileeffectiverights53\_\_item 52](#_Toc314686030)

[2.29. win-def:printereffectiverights\_test 57](#_Toc314686031)

[2.29.1. Known Supported Platforms 57](#_Toc314686032)

[2.30. win-def:printereffectiverights\_object 57](#_Toc314686033)

[2.31. win-def:PrinterEffectiveRightsBehaviors 59](#_Toc314686034)

[2.32. win-def:printereffectiverights\_state 61](#_Toc314686035)

[2.33. win-sc:printereffectiverights\_item 63](#_Toc314686036)

[2.34. win-def:accesstoken\_test 65](#_Toc314686037)

[2.34.1. Known Supported Platforms 65](#_Toc314686038)

[2.35. win-def:accesstoken\_object 66](#_Toc314686039)

[2.36. win-def:AccesstokenBehaviors 67](#_Toc314686040)

[2.37. win-def:accesstoken\_state 68](#_Toc314686041)

[2.38. win-sc:accesstoken\_item 75](#_Toc314686042)

[2.39. win-def:auditeventpolicy\_test 81](#_Toc314686043)

[2.39.1. Known Supported Platforms 81](#_Toc314686044)

[2.40. win-def:auditeventpolicy\_object 81](#_Toc314686045)

[2.41. win-def:auditeventpolicy\_state 82](#_Toc314686046)

[2.42. win-sc:auditeventpolicy\_\_item 84](#_Toc314686047)

[2.43. win-def:EntityStateAuditType 86](#_Toc314686048)

[2.44. win-sc:EntityItemAuditType 86](#_Toc314686049)

[2.45. win-def:auditeventpolicysubcategories\_test 87](#_Toc314686050)

[2.45.1. Known Supported Platforms 87](#_Toc314686051)

[2.46. win-def:auditeventpolicysubcategories\_object 87](#_Toc314686052)

[2.47. win-def: auditeventpolicysubcategories\_state 88](#_Toc314686053)

[2.48. win-sc:auditeventpolicysubcategories\_\_item 98](#_Toc314686054)

[2.49. win-def:EntityStateAuditType 108](#_Toc314686055)

[2.50. win-sc:EntityItemAuditType 109](#_Toc314686056)

[2.51. win-def:passwordpolicy\_test 110](#_Toc314686057)

[2.51.1. Known Supported Platforms 110](#_Toc314686058)

[2.52. win-def:passwordpolicy\_object 110](#_Toc314686059)

[2.53. win-def:passwordpolicy\_state 111](#_Toc314686060)

[2.54. win-sc:passwordpolicy\_item 114](#_Toc314686061)

[2.55. win-def:lockoutpolicy\_test 118](#_Toc314686062)

[2.55.1. Known Supported Platforms 118](#_Toc314686063)

[2.56. win-def:lockoutpolicy\_object 118](#_Toc314686064)

[2.57. win-def: lockoutpolicy\_state 119](#_Toc314686065)

[2.58. win-sc: lockoutpolicy \_item 122](#_Toc314686066)

[2.59. win-def:wmi57\_test 124](#_Toc314686067)

[2.59.1. Known Supported Platforms 124](#_Toc314686068)

[2.60. win-def:wmi57\_object 124](#_Toc314686069)

[2.61. win-def: wmi57\_state 126](#_Toc314686070)

[2.62. win-sc:wmi57\_item 127](#_Toc314686071)

[2.63. win-def:sid\_test 128](#_Toc314686072)

[2.63.1. Known Supported Platforms 129](#_Toc314686073)

[2.64. win-def:sid\_object 129](#_Toc314686074)

[2.65. win-def:SidBehaviors 131](#_Toc314686075)

[2.66. win-def:sid\_state 132](#_Toc314686076)

[2.67. win-sc:sid\_item 134](#_Toc314686077)

[2.68. win-def:sid\_sid\_test 135](#_Toc314686078)

[2.68.1. Known Supported Platforms 136](#_Toc314686079)

[2.69. win-def:sid\_sid\_object 136](#_Toc314686080)

[2.70. win-def:SidSidBehaviors 137](#_Toc314686081)

[2.71. win-def:sid\_sid\_state 138](#_Toc314686082)

[2.72. win-sc:sid\_sid\_item 140](#_Toc314686083)

[2.73. win-def:cmdlet\_test 141](#_Toc314686084)

[2.73.1. Known Supported Platforms 141](#_Toc314686085)

[2.74. win-def:cmdlet\_object 142](#_Toc314686086)

[2.75. win-def:cmdlet\_state 145](#_Toc314686087)

[2.76. win-sc:cmdlet\_item 147](#_Toc314686088)

[2.77. win-def:EntityObjectGUIDType 150](#_Toc314686089)

[2.78. win-def:EntityStateGUIDType 150](#_Toc314686090)

[2.79. win-sc:EntityItemGUIDType 151](#_Toc314686091)

[2.80. win-def:EntityObjectCmdletVerbType 151](#_Toc314686092)

[2.81. win-def:EntityStateCmdletVerbType 152](#_Toc314686093)

[2.82. win-sc:EntityItemCmdletVerbType 153](#_Toc314686094)

[2.83. win-def:user\_test 154](#_Toc314686095)

[2.83.1. Known Supported Platforms 154](#_Toc314686096)

[2.84. win-def:user\_object 154](#_Toc314686097)

[2.85. win-def:user\_state 156](#_Toc314686098)

[2.86. win-sc:user\_item 158](#_Toc314686099)

[2.87. win-def:user\_sid55\_test 161](#_Toc314686100)

[2.87.1. Known Supported Platforms 161](#_Toc314686101)

[2.88. win-def:user\_sid55\_object 161](#_Toc314686102)

[2.89. win-def:user\_sid55\_state 162](#_Toc314686103)

[2.90. win-sc:user\_sid\_item 163](#_Toc314686104)

[2.91. win-def:wmi\_test 165](#_Toc314686105)

[2.91.1. Known Supported Platforms 165](#_Toc314686106)

[2.92. win-def:wmi\_object 165](#_Toc314686107)

[2.93. win-def:wmi\_state 167](#_Toc314686108)

[2.94. win-sc:wmi\_item 168](#_Toc314686109)

[2.95. win-def:group\_test 169](#_Toc314686110)

[2.95.1. Known Supported Platforms 170](#_Toc314686111)

[2.96. win-def:group\_object 170](#_Toc314686112)

[2.97. win-def:group\_state 171](#_Toc314686113)

[2.98. win-sc:group\_item 175](#_Toc314686114)

[2.99. win-def:group\_sid\_test 178](#_Toc314686115)

[2.99.1. Known Supported Platforms 178](#_Toc314686116)

[2.100. win-def:group\_sid\_object 179](#_Toc314686117)

[2.101. win-def:group\_sid\_state 180](#_Toc314686118)

[2.102. win-sc:group\_sid\_item 180](#_Toc314686119)

[2.103. win-def:metabase\_test 182](#_Toc314686120)

[2.103.1. Known Supported Platforms 182](#_Toc314686121)

[2.104. win-def:metabase\_object 182](#_Toc314686122)

[2.105. win-def:metabase\_state 184](#_Toc314686123)

[2.106. win-sc:metabase\_item 185](#_Toc314686124)

[2.107. win-def:process\_test 187](#_Toc314686125)

[2.107.1. Known Supported Platforms 187](#_Toc314686126)

[2.108. win-def:process\_object 187](#_Toc314686127)

[2.109. win-def:process\_state 188](#_Toc314686128)

[2.110. win-sc:process\_item 189](#_Toc314686129)

[Appendix A – Normative References 191](#_Toc314686130)

[Appendix B - Change Log 191](#_Toc314686131)

[Appendix C - Terms and Acronyms 191](#_Toc314686132)

# Introduction

## 1.1 Document Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in *RFC 2119* [1].

The following font and font style conventions are used throughout the remainder of this document:

* The Courier New font is used for writing constructs in the OVAL Language Data Model.

Example: generator

* The *'italic, with single quotes'* font is used for noting values for OVAL Language properties.

Example: *'does not exist'*

* The bold font and the keyword **Default Value:** are used to indicate a property's default value.

Example: **Default Value: -1**

* The bold font and the keyword **xsi:nil="true":** are used to indicate the meaning of an entity when the xsi:nil property is set to true.

Example: **xsi:nil="true"** indicates that the file\_object MUST collect the set of directories specified by the path entity. In addition, a value, for the filename entity, MUST NOT be specified.

This document uses the concept of namespaces[[3]](#footnote-3) to logically group OVAL constructs throughout both the Data Model section of the document, as well as other parts of the specification. The format of these namespaces is prefix:element, where the prefix is the namespace component, and the element is the name of the qualified construct. The following table lists the namespaces used in this document:

|  |  |  |  |
| --- | --- | --- | --- |
| Data Model | Namespace | Description | Example |
| OVAL Definitions | oval-def | The OVAL Definitions data model that defines the core framework constructs for creating OVAL Definitions. This is defined in the OVAL Language Specification [2]. | oval-def:TestType |
| OVAL System Characteristics | oval-sc | The OVAL System Characteristics data model, which defines the constructs used to capture the data collected on a target system. This is defined in the OVAL Language Specification. | oval-sc:ItemType |
| Windows Definitions | win-def | The Windows Definitions data model defines the platform-specific constructs used in OVAL Definitions to make assertions about the state of Microsoft Windows systems. | win-def:file\_test |
| Windows System Characteristics | win-sc | The Windows System Characteristics data model defines the platform-specific constructs used in OVAL System Characteristics to represent the system state information collected from Microsoft Windows systems. | win-sc:file\_item |

Lastly, each OVAL Test will contain a section titled "Known Supported Platforms" that specifies which platforms the OVAL Test is known to work on. This section is provided for convenience only and should not be considered a comprehensive list. In addition, there may be further known support restrictions specified for behaviors or entities that supersede the "Known Supported Platforms" section for the OVAL Test.

## 1.2 Document Structure

This document serves as the specification for the Microsoft Windows extension of the OVAL Language Specification and defines the platform-specific data model. This document is organized into the following sections:

* Section 1 – Introduction
* Section 2 – OVAL Language Windows Component Model
* Appendix A – References
* Appendix B – Change Log
* Appendix C – Terms and Acronyms

# OVAL Language Windows Component Model

The OVAL Language Windows Component Data Model is the platform-specific extension of the OVAL Language Data Model for Microsoft Windows operating systems.

## Data Model Conventions

This document follows the data model conventions described in Section 4.1 of the OVAL Language Specification.

## win-def:file\_test

The file\_test is used to make assertions about the system state information associated with the directories and files[[4]](#footnote-4) on file systems supported by Microsoft Windows operating systems. The file\_test MUST reference one file\_object and zero or more file\_states.



### Known Supported Platforms

* Windows XP
* Windows Vista
* Windows 7

## win-def:file\_object

The file\_object construct defines the set of files and/or directories whose associated system state information should be collected and represented as file\_items. The file\_object is capable of collecting directories and all file types as defined in the EntityStateFileTypeType enumeration.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| set | oval-def:set | 0..1 | false | Enables the expression of complex file\_objects that are the result of logically combining and filtering the file\_items that are identified by one or more file\_objects.  The behaviors, filepath, path, filename, and filter properties MUST NOT be specified when this property is specified.  Please see the OVAL Language Specification for additional information. |
| behaviors | win-def:FileBehaviors | 0..1 | false | Specifies the behaviors that direct how the file\_object collects file\_items from the system. |
| filepath | oval-def:  EntityObjectStringType | 0..1 | false | The absolute path to a file on the system.  The absolute path SHOULD align with the guidance provided in the MSDN documentation[[5]](#footnote-5).  A directory MUST NOT be specified for this property.  The path and filename properties MUST NOT be specified when this property is specified.  The max\_depth and recurse\_direction behaviors MUST NOT be used in conjunction with this property as they are reserved for use with the path and filename properties. |
| path | oval-def:  EntityObjectStringType | 0..1 | false | The directory component of the absolute path to a directory or file on the system.  The path component SHOULD align with the guidance provided in the MSDN documentation[[6]](#footnote-6).  The filepath property MUST NOT be specified when this property is specified. |
| filename | oval-def:  EntityObjectStringType | 0..1 | true | The name of a file to evaluate.  A filename MUST NOT contain the characters in the set { /, \, ?, |, >, :, \*}. The filename SHOULD also align with the guidance provided in the MSDN documentation, as there are more conventions when naming files beyond the characters listed above[[7]](#footnote-7).  The filepath property MUST NOT be specified when this property is specified.  **xsi:nil="true"** indicates that the file\_object MUST collect the set of directories specified by the path entity. In addition, a value for the filename entity MUST NOT be specified. |
| Filter | oval-def:filter | 0..\* | false | Allows for the explicit inclusion or exclusion of file\_items from the set of file\_items collected by a file\_object.  Please see the OVAL Language Specification [2] for additional information. |

## win-def:FileBehaviors

The FileBehaviors construct defines the behaviors that direct how the file\_object collects file\_items from the system. Note that using these behaviors may result in some unique results. For example, a double negative type condition might be created where an object entity says include everything except a specific item, but a behavior is used that might then add that item back in.

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute | Type | Possible Values | Description |
| max\_depth | integer | *< -1*  *-1*  *0*  *> 0* | Defines the maximum depth of file system traversal when the recurse\_direction behavior is set to a value other than *'none'*.  *< -1*: not permitted.  *-1***:** traverse the file system with no limitation.  *0***:** do not traverse the file system.  *> 0***:** traverse the file system for the specified number of levels.  **Default Value: -1** |
| recurse\_direction | string | *'none'*  'up'  *'down'* | Defines the direction to recursively visit the directories on the file system.  *'none'*: do not traverse the file system.  'up':traverse the file system by recursively visiting the parent directories.  *'down'*:traverse the file system by recursively visiting the child directories.  An error MUST NOT be reported when the max\_depth behavior specifies a certain level of traversal and that level does not exist.  **Default Value: none** |
| recurse\_file\_system | string | *'all'*  *'local'*  *'defined'* | Defines the file system limitation of any searching. This applies to all operations as specified in the path or filepath entity.  *'all'*:traverse both local and remote file systems.  *'local'*:only traverse the local file systems.  *'defined'*:only traverse the specified file system.  The value of *'defined'* MUST only be used in conjunction with the equality operation because the path or filepath entity must explicitly define a file system.  **Default Value: all** |
| windows\_view | string | *'32\_bit'*  *'64\_bit'* | 64-bit versions of Windows provide an alternate file system view to 32-bit applications[[8]](#footnote-8). This behavior defines which view should be examined by the file\_object.  *'32\_bit'*:check the 32\_bit view of the file system.  *'64\_bit'*:check the 64\_bit view of the file system.  This behavior only applies to 64-bit versions of Windows and MUST NOT be applied on other platforms.  **Default Value: 64-bit** |

## win-def:file\_state

The file\_state construct is used by a file\_test to specify the system state information, associated with files or directories, to check on file systems that are supported by Microsoft Windows platforms.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| filepath | oval-def:EntityStateStringType | 0..1 | false | The absolute path to a file on the system.  The absolute path SHOULD align with the guidance provided in the MSDN documentation[[9]](#footnote-9).  A directory MUST NOT be specified for this property.  The max\_depth and recurse\_direction behaviors MUST NOT be used in conjunction with this property as they are reserved for use with the path and filename properties. |
| Path | oval-def:EntityStateStringType | 0..1 | false | The directory component of the absolute path to a directory or file on the system.  The path component SHOULD align with the guidance provided in the MSDN documentation[[10]](#footnote-10). |
| filename | oval-def:EntityStateStringType | 0..1 | false | The name of a file to evaluate.  A filename MUST NOT contain the characters in the set { /, \, ?, |, >, :, \*}. The filename SHOULD also align with the guidance provided in the MSDN documentation, as there are more conventions when naming files beyond the characters listed above[[11]](#footnote-11). |
| owner | oval-def:EntityStateStringType | 0..1 | false | The owner of the file.  The owner MUST BE expressed in the DOMAIN\username format.  The username component of the owner can be retrieved using the GetSecurityInfo function[[12]](#footnote-12) and the domain component can be retrieved using the LookupAccountSid function[[13]](#footnote-13). |
| Size | oval-def:EntityStateIntType | 0..1 | false | The size of the file in bytes.  The size of the file can be retrieved using the \_stat function[[14]](#footnote-14) or GetFileSizeEx function[[15]](#footnote-15). |
| a\_time | oval-def:EntityStateIntType | 0..1 | false | The date and time that the file was last accessed.  This is valid on NTFS formatted disk drives, but, not on FAT formatted disk drives.  This value MUST align with the FILETIME structure which contains a 64-bit number representing how many 100-nanosecond intervals have passed since January 1, 1601 (UTC)[[16]](#footnote-16).  The GetFileTime function[[17]](#footnote-17) can retrieve the last accessed time. |
| c\_time | oval-def:EntityStateIntType | 0..1 | false | The date and time that the file was created.  This is valid on NTFS formatted disk drives, but, not on FAT formatted disk drives.  This value MUST align with the FILETIME structure which contains a 64-bit number representing how many 100-nanosecond intervals have passed since January 1, 1601 (UTC)[[18]](#footnote-18).  The GetFileTime function[[19]](#footnote-19) can retrieve the creation time. |
| m\_time | oval-def:EntityStateIntType | 0..1 | false | The date and time that the file was last modified.  This value MUST align with the FILETIME structure which contains a 64-bit number representing how many 100-nanosecond intervals have passed since January 1, 1601 (UTC)[[20]](#footnote-20).  The GetFileTime function[[21]](#footnote-21) can retrieve the last modified time. |
| ms\_checksum | oval-def:EntityStateStringType | 0..1 | false | The checksum of the file.  The checksum MUST align with the value supplied by Microsoft's MapFileAndCheckSum function[[22]](#footnote-22). |
| version | oval-def:  EntityStateVersionType | 0..1 | false | The version number of the file.  This value can be obtained via the VarQueryValue function[[23]](#footnote-23) or the FileVersionInfo class[[24]](#footnote-24). |
| type | win-def:  EntityStateFileTypeType | 0..1 | false | The type of the file.  This value can be obtained using the GetFileType function[[25]](#footnote-25) with the exception of FILE\_ATTRIBUTE\_DIRECTORY which can be obtained with the GetFileAttributesEx function[[26]](#footnote-26). |
| development\_class | oval-def:EntityStateStringType | 0..1 | false | The development environment in which the file was created.  The current development environments are the general distribution releases (GDR) development environment and the quick fix engineering (QFE) development environment.  This value MUST be the text prior to the mmmmmm-nnnn component of the file version formats[[27]](#footnote-27).  This value can be obtained via the VarQueryValue function[[28]](#footnote-28). |
| company | oval-def:EntityStateStringType | 0..1 | false | The name of the company that created the file.  This value can be obtained via the VarQueryValue function[[29]](#footnote-29) or the FileVersionInfo class[[30]](#footnote-30). |
| internal\_name | oval-def:EntityStateStringType | 0..1 | false | The internal name of the file.  This value can be obtained via the VarQueryValue function[[31]](#footnote-31) or the FileVersionInfo class[[32]](#footnote-32). |
| language | oval-def:EntityStateStringType | 0..1 | false | The description string for the Microsoft Language Identifier associated with the file.  This value can be obtained via the VarQueryValue function[[33]](#footnote-33) or the FileVersionInfo class[[34]](#footnote-34). |
| original\_filename | oval-def:EntityStateStringType | 0..1 | false | The original name of the file when it was created.  This value can be obtained via the VarQueryValue function[[35]](#footnote-35) or the FileVersionInfo class[[36]](#footnote-36). |
| product\_name | oval-def:EntityStateStringType | 0..1 | false | The name of the product that the file is distributed with.  This value can be obtained via the VarQueryValue function[[37]](#footnote-37) or the FileVersionInfo class[[38]](#footnote-38). |
| product\_version | oval-def:  EntityStateVersionType | 0..1 | false | The version of the product that the file is distributed with.  This value can be obtained via the VarQueryValue function[[39]](#footnote-39) or the FileVersionInfo class[[40]](#footnote-40). |
| windows\_view | win-def:  EntityStateWindowsViewType | 0..1 | false | The targeted file system view[[41]](#footnote-41) where the file or directory was collected. |

## win-sc:file\_item

The file\_item construct defines the system state information associated with files and directories on file systems supported by the Microsoft Windows platform.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| filepath | oval-sc:  EntityItemStringType | 0..1 | false | The absolute path to a file on the system.  The absolute path SHOULD align with the guidance provided in the MSDN documentation[[42]](#footnote-42).  A directory MUST NOT be specified for this property.  The max\_depth and recurse\_direction behaviors MUST NOT be used in conjunction with this property as they are reserved for use with the path and filename properties. |
| path | oval-sc:  EntityItemStringType | 0..1 | false | The directory component of the absolute path to a directory or file on the system.  The path component SHOULD align with the guidance provided in the MSDN documentation[[43]](#footnote-43). |
| filename | oval-sc:  EntityItemStringType | 0..1 | true | The name of a file to evaluate.  A filename MUST NOT contain the characters in the set { /, \, ?, |, >, :, \*}. The filename SHOULD also align with the guidance provided in the MSDN documentation, as there are more conventions when naming files beyond the characters listed above[[44]](#footnote-44).  **xsi:nil="true"** MUST be set when the filename entity, in the collecting file\_object, has xsi:nil="true" set. In addition, the status of this entity MUST be *'not collected'* and a value for this entity MUST NOT be specified. |
| owner | oval-sc:  EntityItemStringType | 0..1 | false | The owner of the file.  The owner MUST BE expressed in the DOMAIN\username format.  The username component of the owner can be retrieved using the GetSecurityInfo function[[45]](#footnote-45) and the domain component can be retrieved using the LookupAccountSid function[[46]](#footnote-46). |
| size | oval-sc:EntityItemIntType | 0..1 | false | The size of the file in bytes.  The size of the file can be retrieved using the \_stat function[[47]](#footnote-47) or GetFileSizeEx function[[48]](#footnote-48). |
| a\_time | oval-sc:EntityItemIntType | 0..1 | false | The date and time that the file was last accessed.  This is valid on NTFS formatted disk drives, but, not on FAT formatted disk drives.  This value MUST align with the FILETIME structure which contains a 64-bit number representing how many 100-nanosecond intervals have passed since January 1, 1601 (UTC)[[49]](#footnote-49).  The GetFileTime function[[50]](#footnote-50) can retrieve the last accessed time. |
| c\_time | oval-sc:EntityItemIntType | 0..1 | false | The date and time that the file was created.  This is valid on NTFS formatted disk drives, but, not on FAT formatted disk drives.  This value MUST align with the FILETIME structure which contains a 64-bit number representing how many 100-nanosecond intervals have passed since January 1, 1601 (UTC)[[51]](#footnote-51).  The GetFileTime function[[52]](#footnote-52) can retrieve the creation time. |
| m\_time | oval-sc:EntityItemIntType | 0..1 | false | The date and time that the file was last modified.  This value MUST align with the FILETIME structure which contains a 64-bit number representing how many 100-nanosecond intervals have passed since January 1, 1601 (UTC)[[53]](#footnote-53).  The GetFileTime function[[54]](#footnote-54) can retrieve the last modified time. |
| ms\_checksum | oval-sc:  EntityItemStringType | 0..1 | false | The checksum of the file.  The checksum MUST align with the value supplied by Microsoft's MapFileAndCheckSum function[[55]](#footnote-55). |
| version | oval-sc:  EntityItemVersionType | 0..1 | false | The version number of the file.  This value can be obtained via the VarQueryValue function[[56]](#footnote-56) or the FileVersionInfo class[[57]](#footnote-57). |
| type | win-sc:  EntityItemFileTypeType | 0..1 | false | The type of the file.  This value can be obtained using the GetFileType function[[58]](#footnote-58) with the exception of FILE\_ATTRIBUTE\_DIRECTORY which is obtained by looking at the GetFileAttributesEx function[[59]](#footnote-59). |
| development\_class | oval-sc:  EntityItemStringType | 0..1 | false | The development environment in which the file was created.  The current development environments are the general distribution releases (GDR) development environment and the quick fix engineering (QFE) development environment.  This value MUST be the text prior to the mmmmmm-nnnn component of the file version formats[[60]](#footnote-60).  This value can be obtained via the VarQueryValue function[[61]](#footnote-61). |
| company | oval-sc:  EntityItemStringType | 0..1 | false | The name of the company that created the file.  This value can be obtained via the VarQueryValue function[[62]](#footnote-62) or the FileVersionInfo class[[63]](#footnote-63). |
| internal\_name | oval-sc:  EntityItemStringType | 0..1 | false | The internal name of the file.  This value can be obtained via the VarQueryValue function[[64]](#footnote-64) or the FileVersionInfo class[[65]](#footnote-65). |
| language | oval-sc:  EntityItemStringType | 0..1 | false | The description string for the Microsoft Language Identifier associated with the file.  This value can be obtained via the VarQueryValue function[[66]](#footnote-66) or the FileVersionInfo class[[67]](#footnote-67). |
| original\_filename | oval-sc:  EntityItemStringType | 0..1 | false | The original name of the file when it was created.  This value can be obtained via the VarQueryValue function[[68]](#footnote-68) or the FileVersionInfo class[[69]](#footnote-69). |
| product\_name | oval-sc:  EntityItemStringType | 0..1 | false | The name of the product that the file is distributed with.  This value can be obtained via the VarQueryValue function[[70]](#footnote-70) or the FileVersionInfo class[[71]](#footnote-71). |
| product\_version | oval-sc:  EntityItemVersionType | 0..1 | false | The version of the product that the file is distributed with.  This value can be obtained via the VarQueryValue function[[72]](#footnote-72) or the FileVersionInfo class[[73]](#footnote-73). |
| windows\_view | win-sc:  EntityItemWindowsViewType | 0..1 | false | The targeted file system view[[74]](#footnote-74) where the file or directory was collected. |

## win-def:EntityStateFileTypeType

The EntityStateFileTypeType defines the enumeration of possible file types for file systems supported on Microsoft Windows platforms.

|  |  |
| --- | --- |
| Enumeration Value | Description |
| FILE\_ATTRIBUTE\_ DIRECTORY | This value indicates a directory. |
| FILE\_TYPE\_CHAR | This value indicates a character file, typically an LPT device or a console. |
| FILE\_TYPE\_DISK | This value indicates a disk file. |
| FILE\_TYPE\_PIPE | This value indicates a socket, a named pipe, or an anonymous pipe. |
| FILE\_TYPE\_REMOTE | This value is currently unused by Microsoft. |
| FILE\_TYPE\_UNKNOWN | This value indicates that the type of file is unknown. |
| *<empty string>* | This value indicates that no value has been specified and is permitted here to allow for an empty entity which is associated with a reference to an OVAL Variable. |

## win-sc:EntityItemFileTypeType

The EntityItemFileTypeType defines the enumeration of possible file types for file systems supported on Microsoft Windows platforms.

|  |  |
| --- | --- |
| Enumeration Value | Description |
| FILE\_ATTRIBUTE\_DIRECTORY | This value indicates a directory. |
| FILE\_TYPE\_CHAR | This value indicates a character file, typically an LPT device or a console. |
| FILE\_TYPE\_DISK | This value indicates a disk file. |
| FILE\_TYPE\_PIPE | This value indicates a socket, a named pipe, or an anonymous pipe. |
| FILE\_TYPE\_REMOTE | This value is currently unused by Microsoft. |
| FILE\_TYPE\_UNKNOWN | This value indicates that the type of file is unknown. |
| *<empty string>* | This value indicates that no value has been specified and is permitted here to allow for an empty entity which is associated with error and not collected conditions. |

## win-def:EntityStateWindowsViewType

The EntityStateWindowsViewType defines the enumeration of possible views associated with 64-bit Microsoft Windows platforms.

|  |  |
| --- | --- |
| Enumeration Value | Description |
| 32\_bit | This value indicates the 32-bit view. |
| 64\_bit | This value indicates the 64-bit view. |
| *<empty string>* | This value indicates that no value has been specified and is permitted here to allow for an empty entity which is associated with a reference to an OVAL Variable. |

## win-sc:EntityItemWindowsViewType

The EntityItemWindowsViewType defines the enumeration of possible views associated with 64-bit Microsoft Windows platforms.

|  |  |
| --- | --- |
| Enumeration Value | Description |
| 32\_bit | This value indicates the 32-bit view. |
| 64\_bit | This value indicates the 64-bit view. |
| *<empty string>* | This value indicates that no value has been specified and is permitted here to allow for an empty entity which is associated with error and not collected conditions. |

## win-def:registry\_test

The registry\_test is used to make assertions about information associated with the hives and keys in the registry[[75]](#footnote-75) on Microsoft Windows operating systems. The registry\_test MUST reference one registry\_object and zero or more registry\_states.  


### Known Supported Platforms

* Windows XP
* Windows Vista
* Windows 7

## win-def:registry\_object

The registry\_object construct defines the set of keys and/or hives whose associated system state information should be collected and represented as registry\_items. The registry\_object is capable of collecting the hives defined in the win-def:EntityObjectRegistryHiveTypeType enumeration, their keys, and all values whose type is defined in the win-def:EntityObjectRegistryTypeType.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| set | oval-def:set | 0..1 | false | Enables the expression of complex registry\_objects that are the result of logically combining and filtering the registry\_items that are identified by one or more registry\_objects.  The behaviors, hive, key, name, and filter properties MUST NOT be specified when this property is specified.  Please see the OVAL Language Specification [2] for additional information. |
| behaviors | win-def:RegistryBehaviors | 0..1 | false | Specifies the behaviors that direct how the registry\_object collects registry\_items from the system. |
| hive | win-def:  EntityObjectRegistryHiveType | 0..1 | false | The hive that the registry key belongs to.  This SHOULD align with the guidance provided in the MSDN documentation[[76]](#footnote-76). |
| key | oval-def:  EntityObjectStringType | 1..1 | true | The registry key to be collected.  This property MUST NOT include the hive as it must be specified in the hive property.  **xsi:nil="true"** indicates that the registry\_object must collect the set of hives specified by the hive entity. In addition, a value MUST NOT be specified and the name property MUST have xsi:nil="true". |
| name | oval-def:  EntityObjectStringType | 1..1 | true | The name assigned to a value associated with a specific registry key.  If an empty string is specified, the registry key's default value MUST be collected.  **xsi:nil="true"** indicates that the registry\_object must collect the registry\_items specified by the hive and key properties. In addition, a value MUST NOT be specified. |
| filter | oval-def:filter [2] | 0..\* | false | Allows for the explicit inclusion or exclusion of registry\_items from the set of registry\_items collected by a registry\_object.  Please see the OVAL Language Specification [2] for additional information. |

## win-def:RegistryBehaviors

The RegistryBehaviors construct defines the behaviors that direct how the registry\_object collects registry\_items from the system. Note that using these behaviors may result in some unique results. For example, a double negative type condition might be created where an object entity says include everything except a specific item, but a behavior is used that might then add that item back in.

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute | Type | Possible Values | Description |
| max\_depth | integer | *< -1*  *-1*  *0*  *> 0* | Defines the maximum depth of registry traversal when the recurse\_direction behavior is set to a value other than *'none'*.  *< -1*: not permitted.  *-1***:** traverse the registry with no limitation.  *0***:** do not traverse the registry.  *> 0***:** traverse the registry for the specified number of levels.  **Default Value: -1** |
| recurse\_direction | string | *'none'*  'up'  *'down'* | Defines the direction to recursively visit the registry.  *'none'*: do not traverse the registry.  'up':traverse the registry by recursively visiting the parent keys.  *'down'*:traverse the registry by recursively visiting the child keys.  Note: It is not an error if max\_depth specifies a certain level of traversal and that level does not exist.  **Default Value: none** |
| windows\_view | string | *'32\_bit'*  *'64\_bit'* | 64-bit versions of Windows provide an alternate registry view to 32-bit applications[[77]](#footnote-77). This behavior defines which view should be examined by the registry\_object.  *'32\_bit'*:check the 32\_bit view of the registry.  *'64\_bit'*:check the 64\_bit view of the registry.  This behavior only applies to 64-bit versions of Windows and MUST NOT be applied on other platforms.  **Default Value: 64-bit** |

## win-def:registry\_state

The registry\_state construct is used by a registry\_test to specify the system state information, associated with hives or keys, to check in the registry on Microsoft Windows platforms.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| hive | win-def:  EntityStateRegistryHiveType | 0..1 | false | The hive that the registry key belongs to.  This SHOULD align with the guidance provided in the MSDN documentation, which contains the list of predefined hives[[78]](#footnote-78). |
| key | oval-def:  EntityStateStringType | 0..1 | false | The registry key to be collected.  This property MUST NOT include the hive as it must be specified in the hive property. |
| name | oval-def:  EntityStateStringType | 0..1 | false | The name assigned to a value associated with a specific registry key.  If an empty string is specified, the registry key's default value MUST be collected.  This can be obtained using the RegQueryValueEx function[[79]](#footnote-79). |
| last\_write\_time | oval-def:EntityStateIntType | 0..1 | false | The date and time that the key or any of its value entries were modified.  This value MUST align with the FILETIME structure which contains a 64-bit number representing how many 100-nanosecond intervals have passed since January 1, 1601 (UTC)[[80]](#footnote-80).  Last write time can be queried on any key, with hives being classified as a type of key.  When collecting only information about a registry hive or key the last write time will  be the time the key or any of its entries were modified. When collecting only information  about a registry name the last write time will be the time the containing key was modified.  Thus when collecting information about a registry name, the last write time does not correlate  directly to the specified name.  This can be obtained using the RegQueryInfoKey function[[81]](#footnote-81). |
| type | win-def:  EntityStateRegistryTypeType | 0..1 | false | The type associated with the value of a hive or registry key.  This can be obtained using the RegQueryValueEx function[[82]](#footnote-82). |
| value | oval-def:  EntityStateAnySimpleType | 0..\* | false | The value(s) associated with a hive or registry key.  The value of a hive or registry key can be obtained using the RegQueryValueEx function[[83]](#footnote-83).  Please see the OVAL Language Specification [2] for more information about how datatypes are assigned to OVAL Item Entities. |
| windows\_view | win-def:  EntityStateWindowsViewType | 0..1 | false | The targeted registry view[[84]](#footnote-84) where the hive or registry key was collected. |

## win-sc:registry\_item

The registry\_item construct specifies information that can be collected about a particular hive or registry key on a Windows system.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| hive | win-sc:  EntityItemRegistryHiveType | 0..1 | false | The hive that the registry key belongs to.  This SHOULD align with the guidance provided in the MSDN documentation, which contains the list of predefined hives[[85]](#footnote-85). |
| key | oval-sc:EntityItemStringType | 0..1 | true | The registry key to be collected.  This property MUST NOT include the hive as it must be specified in the hive property. |
| name | oval-sc:EntityItemStringType | 0..1 | true | The name assigned to a value associated with a specific registry key.  If an empty string is specified, the registry key's default value MUST be collected.  This can be obtained using the RegQueryValueEx function[[86]](#footnote-86). |
| last\_write\_time | oval-sc:EntityItemIntType | 0..1 | false | The date and time that the key or any of its value entries were last modified.  This value MUST align with the FILETIME structure which contains a 64-bit number representing how many 100-nanosecond intervals have passed since January 1, 1601 (UTC)[[87]](#footnote-87).  Last write time can be queried on any key, with hives being classified as a type of key.  When collecting only information about a registry hive or key the last write time will  be the time the key or any of its entries were modified. When collecting only information  about a registry name the last write time will be the time the containing key was modified.  Thus when collecting information about a registry name, the last write time does not correlate  directly to the specified name.  This can be obtained using the RegQueryInfoKey function[[88]](#footnote-88). |
| type | win-sc:  EntityItemRegistryTypeType | 0..1 | false | The type associated with the value of a hive or registry key.  This can be obtained using the RegQueryValueEx function[[89]](#footnote-89). |
| value | oval-sc:  EntityItemAnySimpleType | 0..\* | false | The value(s) associated with a hive or registry key.  The value of a hive or registry key can be obtained using the RegQueryValueEx function[[90]](#footnote-90).  Please see the OVAL Language Specification [2] for more information about how datatypes are assigned to OVAL Item Entities. |
| windows\_view | win-sc:  EntityItemWindowsViewType | 0..1 | false | The targeted registry view[[91]](#footnote-91) where the hive or registry key was collected. |

## win-def:EntityObjectRegistryHiveType

The EntityObjectRegistryHiveType defines the enumeration of possible hive types for the registry supported on Microsoft Windows platforms[[92]](#footnote-92).

|  |  |
| --- | --- |
| Enumeration Value | Description |
| HKEY\_CLASSES\_ROOT | This value indicates file types with programs and configuration data for automation (e.g. COM objects and Visual Basic Programs). |
| HKEY\_CURRENT\_CONFIG | This value indicates configuration data for the current hardware profile. |
| HKEY\_CURRENT\_USER | This value indicates the user profile of the user that is currently logged into the system. |
| HKEY\_LOCAL\_MACHINE | This value indicates information about the local system. |
| HKEY\_USERS | This value indicates user-specific data. |
| *<empty string>* | This value indicates that no value has been specified and is permitted here to allow for an empty entity which is associated with a reference to an OVAL Variable. |

## win-def:EntityStateRegistryHiveType

The EntityStateRegistryHiveType defines the enumeration of possible hive types for the registry supported on Microsoft Windows platforms[[93]](#footnote-93).

|  |  |
| --- | --- |
| Enumeration Value | Description |
| HKEY\_CLASSES\_ROOT | This value indicates file types with programs and configuration data for automation (e.g. COM objects and Visual Basic Programs). |
| HKEY\_CURRENT\_CONFIG | This value indicates configuration data for the current hardware profile. |
| HKEY\_CURRENT\_USER | This value indicates the user profile of the user that is currently logged into the system. |
| HKEY\_LOCAL\_MACHINE | This value indicates information about the local system. |
| HKEY\_USERS | This value indicates user-specific data. |
| *<empty string>* | This value indicates that no value has been specified and is permitted here to allow for an empty entity which is associated with a reference to an OVAL Variable. |

## win-sc:EntityItemRegistryHiveType

The EntityItemRegistryHiveType defines the enumeration of possible hive types for the registry supported on Microsoft Windows platforms[[94]](#footnote-94).

|  |  |
| --- | --- |
| Enumeration Value | Description |
| HKEY\_CLASSES\_ROOT | This value indicates file types with programs and configuration data for automation (e.g. COM objects and Visual Basic Programs). |
| HKEY\_CURRENT\_CONFIG | This value indicates configuration data for the current hardware profile. |
| HKEY\_CURRENT\_USER | This value indicates the user profile of the user that is currently logged into the system. |
| HKEY\_LOCAL\_MACHINE | This value indicates information about the local system. |
| HKEY\_USERS | This value indicates user-specific data. |
| *<empty string>* | This value indicates that no value has been specified and is permitted here to allow for an empty entity which is associated with error and not collected conditions. |

## win-def:EntityStateRegistryTypeType

The EntityStateRegistryTypeType defines the types[[95]](#footnote-95) associated with the values of hives and registry keys in the registry on Microsoft Windows platforms.

|  |  |
| --- | --- |
| Enumeration Value | Description |
| reg\_binary | This value indicates binary data in any form. |
| reg\_dword | This value indicates a 32-bit number. |
| reg\_expand\_sz | This value indicates a null-terminated string that contains unexpanded references to environment variables. |
| reg\_multi\_sz | This value indicates an array of null-terminated strings, terminated by two null characters. |
| reg\_none | This value indicates no defined value type. |
| reg\_qword | This value indicates a 64-bit number. |
| reg\_sz | This value indicates a single null-terminated string. |
| *<empty string>* | This value indicates that no value has been specified and is permitted here to allow for an empty entity which is associated with a reference to an OVAL Variable. |

## win-sc:EntityItemRegistryTypeType

The EntityItemRegistryTypeType defines the types[[96]](#footnote-96) associated with the values of hives and registry keys in the registry on Microsoft Windows platforms.

|  |  |
| --- | --- |
| Enumeration Value | Description |
| reg\_binary | This value indicates binary data in any form. |
| reg\_dword | This value indicates a 32-bit number. |
| reg\_expand\_sz | This value indicates a null-terminated string that contains unexpanded references to environment variables. |
| reg\_multi\_sz | This value indicates an array of null-terminated strings, terminated by two null characters. |
| reg\_none | This value indicates no defined value type. |
| reg\_qword | This value indicates a 64-bit number. |
| reg\_sz | This value indicates a single null-terminated string. |
| *<empty string>* | This value indicates that no value has been specified and is permitted here to allow for an empty entity which is associated with error and not collected conditions. |

## win-def:fileeffectiverights53\_test

The fileeffectiverights53\_test is used to make assertions about the effective rights of files on Microsoft Windows operating systems[[97]](#footnote-97). The fileeffectiverights53\_test MUST reference one fileeffectiverights53\_object and zero or more fileeffectiverights53\_states.  


### Known Supported Platforms

* Windows XP
* Windows Vista
* Windows 7

## win-def:fileeffectiverights53\_object

The fileeffectiverights53\_object construct defines the set of files and directories and the trustee SID(s)[[98]](#footnote-98) whose associated effective rights information should be collected and represented as fileeffectiverights53\_items. The fileeffectiverights53\_object is capable of collecting directiories and all file types as defined in the EntityStateFileTypeType 

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| Set | oval-def:set | 0..1 | false | Enables the expression of complex fileeffectiverights53\_objects that are the result of logically combining and filtering the fileeffectiverights53\_items that are identified by one or more fileeffectiverights53\_objects.  The behaviors, filepath, path, filename, trustee\_sid, and filter properties MUST NOT be specified when this property is specified.  Please see the OVAL Language Specification [2] for additional information. |
| behaviors | win-def:  FileEffectiveRights53Behaviors | 0..1 | false | Specifies the behaviors that direct how the fileeffectiverights53\_object collects fileeffectiverights53\_items from the system. |
| filepath | oval-def:  EntityObjectStringType | 0..1 | false | The absolute path to a file on the system.  The absolute path SHOULD align with the guidance provided in the MSDN documentation[[99]](#footnote-99).  A directory MUST NOT be specified for this property.  The max\_depth and recurse\_direction behaviors MUST NOT be used in conjunction with this property as they are reserved for use with the path and filename properties. |
| path | oval-def:  EntityObjectStringType | 0..1 | false | The directory component of the absolute path to a directory or file on the system.  The path component SHOULD align with the guidance provided in the MSDN documentation[[100]](#footnote-100).  The filepath property MUST NOT be specified when this property is specified. |
| filename | oval-def:  EntityObjectStringType | 0..1 | true | The name of a file to evaluate.  A filename MUST NOT contain the characters in the set { /, \, ?, |, >, :, \*}. The filename SHOULD also align with the guidance provided in the MSDN documentation, as there are more conventions when naming files beyond the characters listed above[[101]](#footnote-101).  **xsi:nil="true"** indicates that the fileeffectiverights53\_object MUST collect the set of directories specified by the path entity. In addition, a value for the filename entity MUST NOT be specified. |
| trustee\_sid | oval-def:  EntityObjectStringType | 1..1 | false | The unique security identifier associated with a user account, group account, or logon session.  If an operation other than equals is used to identify the matching trustees, then the resulting matches MUST be limited to the trustees explicitly referenced in the file or directory's security descriptor[[102]](#footnote-102). |
| filter | oval-def:filter | 0..\* | false | Allows for the explicit inclusion or exclusion of fileeffectiverights53\_items from the set of fileeffectiverights53\_items collected by a fileeffectiverights53\_object.  Please see the OVAL Language Specification [2] for additional information. |

## FileEffectiveRights53Behaviors

The FileEffectiveRights53Behaviors construct defines the behaviors that direct how the fileeffectiverights53\_object collects fileeffectiverights53\_items from the system. Note that using these behaviors may result in some unique results. For example, a double negative type condition might be created where an object entity says include everything except a specific item, but a behavior is used that might then add that item back in.Also note that FileEffectsRights53Behaviors construct extends the FileBehaviors construct so the max\_depth and recurse\_direction behaviors are not listed here.



|  |  |  |  |
| --- | --- | --- | --- |
| Attribute | Type | Possible Values | Description |
| include\_group | boolean | *'true'*  *'false'* | Defines whether or not the group SID should be collected when the trustee\_sid property specifies a group SID.  *'true'*: The group SID MUST be collected when the trustee\_sid property specifies a group SID.  *'false'*: The group SID MUST NOT be collected when the trustee\_sid property specifies a group SID.  **Default Value: true** |
| resolve\_group | boolean | *'true'*  *'false'* | Defines whether or not the members of group SIDs should be resolved and collected.  Note that all child groups should also be resolved and any valid domain accounts that are members should also be included.  The intent of this behavior is to end up with a list of all individual users from that system that make up the group once everything has been resolved.  *'true'*: The members of a group SID MUST be resolved and collected.  'false': The members of a group SID MUST NOT be resolved or collected.  **Default Value: false** |

## win-def:fileeffectiverights53\_state

The fileeffectiverights53\_state construct is used by a fileeffectiverights53\_test to specify the different effective rights that are associated with a trustee\_sid for files and directories on Microsoft Windows platforms. The GetNamedSecurityInfo function can be used to identify various file permissions[[103]](#footnote-103).



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description | |
| filepath | oval-def:  EntityStateStringType | 0..1 | false | The absolute path to a file on the system.  The absolute path SHOULD align with the guidance provided in the MSDN documentation[[104]](#footnote-104).  A directory MUST NOT be specified for this property.  The max\_depth and recurse\_direction behaviors MUST NOT be used in conjunction with this property as they are reserved for use with the path and filename properties. |
| path | oval-def:  EntityStateStringType | 0..1 | false | The directory component of the absolute path to a directory or file on the system.  The path component SHOULD align with the guidance provided in the MSDN documentation[[105]](#footnote-105).  The filepath property MUST NOT be specified when this property is specified. |
| filename | oval-def:  EntityStateStringType | 0..1 | false | The name of a file to evaluate.  A filename MUST NOT contain the characters in the set { /, \, ?, |, >, :, \*}. The filename SHOULD also align with the guidance provided in the MSDN documentation, as there are more conventions when naming files beyond the characters listed above[[106]](#footnote-106). |
| trustee\_sid | oval-def:  EntityStateStringType | 0..1 | false | The unique security identifier associated with a user account, group account, or logon session.  If an operation other than equals is used to identify the matching trustees, then the resulting matches MUST be limited to the trustees explicitly referenced in the file or directory's security descriptor[[107]](#footnote-107). |
| standard\_delete | oval-def:  EntityStateBoolType | 0..1 | false | The right to delete the file[[108]](#footnote-108). |
| standard\_read\_control | oval-def:  EntityStateBoolType | 0..1 | false | The right to read the information in the file's Security Descriptor, not including the information in the system access control list (SACL)[[109]](#footnote-109). |
| standard\_write\_dac | oval-def:  EntityStateBoolType | 0..1 | false | The right to modify the DACL in the file's Security Descriptor[[110]](#footnote-110). |
| standard\_write\_owner | oval-def:  EntityStateBoolType | 0..1 | false | The right to change the owner in the file's Security Descriptor[[111]](#footnote-111). |
| standard\_synchronize | oval-def:  EntityStateBoolType | 0..1 | false | The right to use the file for synchronization. This enables a thread to wait until the file is in the signaled state[[112]](#footnote-112). |
| access\_system\_security | oval-def:  EntityStateBoolType | 0..1 | false | Indicates access to a system access control list (SACL)[[113]](#footnote-113). |
| generic\_read | oval-def:  EntityStateBoolType | 0..1 | false | Read access[[114]](#footnote-114). |
| generic\_write | oval-def:  EntityStateBoolType | 0..1 | false | Write access[[115]](#footnote-115). |
| generic\_execute | oval-def:  EntityStateBoolType | 0..1 | false | Execute access [[116]](#footnote-116). |
| generic\_all | oval-def:  EntityStateBoolType | 0..1 | false | Read, write, and execute access[[117]](#footnote-117). |
| file\_read\_data | oval-def:  EntityStateBoolType | 0..1 | false | Grants the right to read data from the file, or if a directory, grants the right to list the contents of the directory[[118]](#footnote-118). |
| file\_write\_data | oval-def:  EntityStateBoolType | 0..1 | false | Grants the right to write data to the file, or if a directory, grants the right to add a file to the directory[[119]](#footnote-119). |
| file\_append\_data | oval-def:  EntityStateBoolType | 0..1 | false | Grants the right to append data to the file, or if a directory, grants the right to add a sub-directory to the directory[[120]](#footnote-120). |
| file\_read\_ea | oval-def:  EntityStateBoolType | 0..1 | false | Grants the right to read extended attribute[[121]](#footnote-121). |
| file\_write \_ea | oval-def:  EntityStateBoolType | 0..1 | false | Grants the right to write extended attributes[[122]](#footnote-122). |
| file\_execute | oval-def:  EntityStateBoolType | 0..1 | false | Grants the right to execute a file, or if a directory, the right to traverse the directory[[123]](#footnote-123). |
| file\_delete\_child | oval-def:  EntityStateBoolType | 0..1 | false | Right to delete a directory and all the files it contains (its children), even if the files are read-only[[124]](#footnote-124). |
| file\_read\_attributes | oval-def: EntityStateBoolType | 0..1 | false | Grants the right to read file, or directory, attributes[[125]](#footnote-125). |
| file\_write\_attributes | oval-def:  EntityStateBoolType | 0..1 | false | Grants the right to change file, or directory, attributes[[126]](#footnote-126). |
| windows\_view | win-def:  EntityStateWindowsViewType | 0..1 | false | The targeted file system view[[127]](#footnote-127) where the file or directory was collected. |

## win-sc:fileeffectiverights53\_item

The fileeffectiverights53\_item construct stores the effective rights of a file that a discretionary access control list (DACL) structure grants to a specified trustee.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| filepath | oval-sc:  EntityItemStringType | 0..1 | false | The absolute path to a file on the system.  The absolute path SHOULD align with the guidance provided in the MSDN documentation[[128]](#footnote-128).  A directory MUST NOT be specified for this property.  The max\_depth and recurse\_direction behaviors MUST NOT be used in conjunction with this property as they are reserved for use with the path and filename properties. |
| path | oval-sc:  EntityItemStringType | 0..1 | false | The directory component of the absolute path to a directory or file on the system.  The path component SHOULD align with the guidance provided in the MSDN documentation[[129]](#footnote-129).  The filepath property MUST NOT be specified when this property is specified. |
| filename | oval-sc:  EntityItemStringType | 0..1 | true | The name of a file to evaluate.  A filename MUST NOT contain the characters in the set { /, \, ?, |, >, :, \*}. The filename SHOULD also align with the guidance provided in the MSDN documentation, as there are more conventions when naming files beyond the characters listed above[[130]](#footnote-130). |
| trustee\_sid | oval-sc:  EntityItemStringType | 0..1 | false | The unique security identifier associated with a user account, group account, or logon session.  If an operation other than equals is used to identify the matching trustees, then the resulting matches MUST be limited to the trustees explicitly referenced in the file or directory's security descriptor[[131]](#footnote-131). |
| standard\_delete | oval-sc:EntityItemBoolType | 0..1 | false | The right to delete the file[[132]](#footnote-132). |
| standard\_read\_control | oval-sc:EntityItemBoolType | 0..1 | false | The right to read the information in the file's Security Descriptor, not including the information in the system access control list (SACL)[[133]](#footnote-133). |
| standard\_write\_dac | oval-sc:EntityItemBoolType |  |  | The right to modify the DACL in the file's Security Descriptor[[134]](#footnote-134). |
| standard\_write\_owner | oval-sc:EntityItemBoolType | 0..1 | false | The right to change the owner in the file's Security Descriptor[[135]](#footnote-135). |
| standard\_synchronize | oval-sc:EntityItemBoolType | 0..1 | false | The right to use the file for synchronization. This enables a thread to wait until the file is in the signaled state[[136]](#footnote-136). |
| access\_system\_security | oval-sc:EntityItemBoolType | 0..1 | false | Indicates access to a system access control list (SACL)[[137]](#footnote-137). |
| generic\_read | oval-sc:EntityItemBoolType | 0..1 | false | Read access[[138]](#footnote-138). |
| generic\_write | oval-sc:EntityItemBoolType | 0..1 | false | Write access[[139]](#footnote-139). |
| generic\_execute | oval-sc:EntityItemBoolType | 0..1 | false | Execute access [[140]](#footnote-140). |
| generic\_all | oval-sc:EntityItemBoolType | 0..1 | false | Read, write, and execute access[[141]](#footnote-141). |
| file\_read\_data | oval-sc:EntityItemBoolType | 0..1 | false | Grants the right to read data from the file, or if a directory, grants the right to list the contents of the directory[[142]](#footnote-142). |
| file\_write\_data | oval-sc:EntityItemBoolType | 0..1 | false | Grants the right to write data to the file, or if a directory, grants the right to add a file to the directory[[143]](#footnote-143). |
| file\_append\_data | oval-sc:EntityItemBoolType | 0..1 | false | Grants the right to append data to the file, or if a directory, grants the right to add a sub-directory to the directory[[144]](#footnote-144). |
| file\_read\_ea | oval-sc:EntityItemBoolType | 0..1 | false | Grants the right to read extended attribute[[145]](#footnote-145). |
| file\_write \_ea | oval-sc:EntityItemBoolType | 0..1 | false | Grants the right to write extended attributes[[146]](#footnote-146). |
| file\_execute | oval-sc:EntityItemBoolType | 0..1 | false | Grants the right to execute a file, or if a directory, the right to traverse the directory[[147]](#footnote-147). |
| file\_delete\_child | oval-sc:EntityItemBoolType | 0..1 | false | Right to delete a directory and all the files it contains (its children), even if the files are read-only[[148]](#footnote-148). |
| file\_read\_attributes | oval-sc:EntityItemBoolType | 0..1 | false | Grants the right to read file, or directory, attributes[[149]](#footnote-149). |
| file\_write\_attributes | oval-sc:EntityItemBoolType | 0..1 | false | Grants the right to change file, or directory, attributes[[150]](#footnote-150). |
| windows\_view | win-sc:  EntityItemWindowsViewType | 0..1 | false | The targeted file system view[[151]](#footnote-151) where the file or directory was collected. |

## win-def:printereffectiverights\_test

The printereffectiverights\_test is used to make assertions about the effective rights of Windows printers[[152]](#footnote-152). The printereffectiverights53\_test MUST reference one printereffectiverights53\_object and zero or more printereffectiverights53\_states.  


### Known Supported Platforms

* Windows XP
* Windows Vista
* Windows 7

## win-def:printereffectiverights\_object

The printereffectiverights\_object construct defines the set of printers and SIDs[[153]](#footnote-153) whose associated system state information should be collected and represented as printereffectiverights\_items. The printer represents the printer to be evaluated while the trustee SID represents the account (SID) to check effective rights of. If multiple printers or SIDs are matched by either reference then each possible combination of file and SID is a matching printer effective rights object. 

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| set | oval-def:set | 0..1 | false | Enables the expression of complex printereffectiverights\_objects that are the result of logically combining and filtering the printereffectiverights\_items that are identified by one or more printereffectiverights \_objects. |
| behaviors | win-def:  PrinterEffectiveRightsBehaviors | 0..1 | false | Specifies the behaviors that direct how the printereffectiverights\_object collects printereffectiverights\_items from the system. |
| printer\_name | oval-def:  EntityObjectStringType | 0..1 | false | A printer that a user may have rights on.  The printer name SHOULD align with the guidance provided in the MSDN documentation. |
| trustee\_sid | oval-def:  EntityObjectStringType | 0..1 | true | The unique SID associated with a user, group, system, or program (such as a Windows service).  If an operation other than equals is used to identify matching trustees, such as not equal or pattern match, then the resulting matches SHALL be limited to only the trustees referenced in the printer's Security Descriptor[[154]](#footnote-154). |
| filter | oval-def:filter [2] | 0..\* | false | Allows for the explicit inclusion or exclusion of printereffectiverights\_items from the set of printereffectiverights\_items collected by a printereffectiverights\_object.  Please see the OVAL Language Specification [2] for additional information. |

## win-def:PrinterEffectiveRightsBehaviors

The PrinterEffectiveRightsBehaviors construct defines the behaviors that direct how the printereffectiverights\_object collects printereffectiverights\_items from the system. Note that using these behaviors may result in some unique results. For example, a double negative type condition might be created where an object entity says include everything except a specific item, but a behavior is used that might then add that item back in.Also note that PrinterEffectiveRightsBehaviors extends FileBehaviors so attributes such as max\_depth and recurse\_direction are not listed here.

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute | Type | Possible Values | Description |
| include\_group | bool | *'true'*  *'false'* | Defines whether or not the group SID should be collected when the trustee\_sid property specifies a group SID.  *'true'*: The group SID MUST be collected when the trustee\_sid property specifies a group SID.  *'false'*: The group SID MUST NOT be collected when the trustee\_sid property specifies a group SID.  **Default Value: true** |
| resolve\_group | bool | *'true'*  *'false'* | Defines whether or not the members of group SIDs should be resolved and collected.  Note that all child groups should also be resolved and any valid domain accounts that are members should also be included.  The intent of this behavior is to end up with a list of all individual users from that system that make up the group once everything has been resolved.  *'true'*: The members of a group SID MUST be resolved and collected.  'false': The members of a group SID MUST NOT be resolved or collected.  **Default Value: false** |

## win-def:printereffectiverights\_state

The printereffectiverights\_state construct is used by a printereffectiverights \_test to specify the different rights that can be associated with a given printereffectiverights\_object under Microsoft Windows platforms.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| printer\_name | oval-def:  EntityStateStringType | 0..1 | false | A printer that a user may have rights on.  The printer name SHOULD align with the guidance provided in the MSDN documentation. |
| trustee\_sid | oval-def:  EntityStateStringType | 0..1 | false | The unique SID associated with a user, group, system, or program (such as a Windows service)[[155]](#footnote-155). |
| standard\_delete | oval-def:  EntityStateBoolType | 0..1 | false | The right to delete the printer object[[156]](#footnote-156). |
| standard\_read\_control | oval-def:  EntityStateBoolType | 0..1 | false | The right to read the information in the printer object's Security Descriptor, not including the information in the system access control list (SACL)[[157]](#footnote-157). |
| standard\_write\_dac | oval-def:  EntityStateBoolType | 0..1 | false | The right to modify the DACL in the printer object's Security Descriptor[[158]](#footnote-158). |
| standard\_write\_owner | oval-def:  EntityStateBoolType | 0..1 | false | The right to change the owner in the printer object's Security Descriptor[[159]](#footnote-159). |
| standard\_synchronize | oval-def:  EntityStateBoolType | 0..1 | false | The right to use the printer object for synchronization. This enables a thread to wait until the file is in the signaled state[[160]](#footnote-160). |
| access\_system\_security | oval-def:  EntityStateBoolType | 0..1 | false | Indicates access to a system access control list (SACL)[[161]](#footnote-161). |
| generic\_read | oval-def:  EntityStateBoolType | 0..1 | false | Read access[[162]](#footnote-162). |
| generic\_write | oval-def:  EntityStateBoolType | 0..1 | false | Write access[[163]](#footnote-163). |
| generic\_execute | oval-def:  EntityStateBoolType | 0..1 | false | Execute access [[164]](#footnote-164). |
| generic\_all | oval-def:  EntityStateBoolType | 0..1 | false | Read, write, and execute access[[165]](#footnote-165). |
| printer\_access\_administer | oval-def:  EntityStateBoolType | 0..1 | false | Access to perform administrative tasks[[166]](#footnote-166), which include pausing the printer, deleting all print jobs, resuming a paused printer, amd setting the printer status[[167]](#footnote-167). |
| printer\_access\_use | oval-def:  EntityStateBoolType | 0..1 | false | Access to perform basic printing operations[[168]](#footnote-168). |
| job\_access\_administer | oval-def:  EntityStateBoolType | 0..1 | false | Printer-specific authorization to cancel, pause, resume, or restart the job[[169]](#footnote-169). |
| job\_access\_read | oval-def:  EntityStateBoolType | 0..1 | false | Printing-specific read rights for the spool file[[170]](#footnote-170). |

## win-sc:printereffectiverights\_item

The printereffectiverights\_item stores the effective rights of a printer that a discretionary access control list (DACL) structure grants to a specified trustee.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| printer\_name | oval-sc:  EntityItemStringType | 0..1 | false | A printer that a user may have rights on.  The printer name SHOULD align with the guidance provided in the MSDN documentation. |
| trustee\_sid | oval-sc:  EntityItemStringType | 0..1 | false | The unique SID associated with a user, group, system, or program (such as a Windows service)[[171]](#footnote-171). |
| standard\_delete | oval-sc:EntityItemBoolType | 0..1 | false | The right to delete the printer object[[172]](#footnote-172). |
| standard\_read\_control | oval-sc:EntityItemBoolType | 0..1 | false | The right to read the information in the printer object's Security Descriptor, not including the information in the system access control list (SACL)[[173]](#footnote-173). |
| standard\_write\_dac | oval-sc:EntityItemBoolType | 0..1 | false | The right to modify the DACL in the printer object's Security Descriptor[[174]](#footnote-174). |
| standard\_write\_owner | oval-sc:EntityItemBoolType | 0..1 | false | The right to change the owner in the printer object's Security Descriptor[[175]](#footnote-175). |
| standard\_synchronize | oval-sc:EntityItemBoolType | 0..1 | false | The right to use the printer object for synchronization. This enables a thread to wait until the file is in the signaled state[[176]](#footnote-176). |
| access\_system\_security | oval-sc:EntityItemBoolType | 0..1 | false | Indicates access to a system access control list (SACL)[[177]](#footnote-177). |
| generic\_read | oval-sc:EntityItemBoolType | 0..1 | false | Read access[[178]](#footnote-178). |
| generic\_write | oval-sc:EntityItemBoolType | 0..1 | false | Write access[[179]](#footnote-179). |
| generic\_execute | oval-sc:EntityItemBoolType | 0..1 | false | Execute access [[180]](#footnote-180). |
| generic\_all | oval-sc:EntityItemBoolType | 0..1 | false | Read, write, and execute access[[181]](#footnote-181). |
| printer\_access\_administer | oval-sc:EntityItemBoolType | 0..1 | false | Access to perform administrative tasks[[182]](#footnote-182), which include pausing the printer, deleting all print jobs, resuming a paused printer, amd setting the printer status[[183]](#footnote-183). |
| printer\_access\_use | oval-sc:EntityItemBoolType | 0..1 | false | Access to perform basic printing operations[[184]](#footnote-184). |
| job\_access\_administer | oval-sc:EntityItemBoolType | 0..1 | false | Printer-specific authorization to cancel, pause, resume, or restart the job[[185]](#footnote-185). |
| job\_access\_read | oval-sc:EntityItemBoolType | 0..1 | false | Printing-specific read rights for the spool file[[186]](#footnote-186). |

## win-def:accesstoken\_test

The accesstoken\_test is used to make assertions about the properties of Windows access tokens as well as individual privileges and rights associated with them[[187]](#footnote-187). The accesstoken\_test MUST reference one accesstoken\_object and zero or more accesstoken\_states.  


### Known Supported Platforms

* Windows XP
* Windows Vista
* Windows 7

## win-def:accesstoken\_object

The accesstoken\_object construct defines the security principal that identifies user, group, or computer account associated with an access token[[188]](#footnote-188), whose associated information should be collected and represented as accesstoken\_items. 

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| set | oval-def:set | 0..1 | false | Enables the expression of complex accesstoken\_objects that are the result of logically combining and filtering the accesstoken\_items that are identified by one or more accesstoken\_objects. |
| behaviors | win-def:  AccesstokenBehaviors | 0..1 | false | Specifies the behaviors that direct how the accesstoken\_object collects accesstoken \_items from the system. |
| security\_principle | oval-def:  EntityObjectStringType | 0..1 | false | The access token being specified. Security principals include users or groups with either local or domain accounts, and computer accounts created when a computer joins a domain.  In Windows, security principals are case-insensitive. As a result, it is recommended that the case-insensitive operations are used for this entity. |
| filter | oval-def:filter [2] | 0..\* | false | Allows for the explicit inclusion or exclusion of accesstoken\_items from the set of accesstoken\_items collected by a accesstoken\_object.  Please see the OVAL Language Specification [2] for additional information. |

## win-def:AccesstokenBehaviors

The AccesstokenBehaviors construct defines the behaviors that direct how the accesstoken\_object collects accesstoken\_items from the system. Note that using these behaviors may result in some unique results. For example, a double negative type condition might be created where an object entity says include everything except a specific item, but a behavior is used that might then add that item back in.

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute | Type | Possible Values | Description |
| include\_group | bool | *'true'*  *'false'* | Defines whether or not the group SID should be collected when the trustee\_sid property specifies a group SID.  *'true'*: The group SID MUST be collected when the trustee\_sid property specifies a group SID.  *'false'*: The group SID MUST NOT be collected when the trustee\_sid property specifies a group SID.  **Default Value: true** |
| resolve\_group | bool | *'true'*  *'false'* | Defines whether or not the members of group SIDs should be resolved and collected.  Note that all child groups should also be resolved and any valid domain accounts that are members should also be included.  The intent of this behavior is to end up with a list of all individual users from that system that make up the group once everything has been resolved.  *'true'*: The members of a group SID MUST be resolved and collected.  'false': The members of a group SID MUST NOT be resolved or collected.  **Default Value: false** |

## win-def:accesstoken\_state

The accesstoken\_state construct is used by an accesstoken\_test to specify the information that can be used to evaluate the specified access tokens associated with a given accesstoken\_object. All attributes ending in "privilege" are considered access token privileges[[189]](#footnote-189), and all attributes ending in "right", with the exception of setrustedcredmanaccessnameright, which is a privilege[[190]](#footnote-190), are access token rights[[191]](#footnote-191).



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| security\_principle | oval-def:  EntityStateStringType | 0..1 | false | Identifies an access token to test for. Security principals include users or groups with either local or domain accounts, and computer accounts created when a computer joins a domain.  In Windows, security principals are case-insensitive. As a result, it is recommended that the case-insensitive operations are used for this entity. |
| seassignprimarytokenprivilege | oval-def:  EntityStateBoolType | 0..1 | false | Gives the user the privilege to replace a process-level token. |
| seauditprivilege | oval-def:  EntityStateBoolType | 0..1 | false | Gives the user the privilege to generate security audits. |
| sebackupprivilege | oval-def:  EntityStateBoolType | 0..1 | false | Gives the user the privilege to back up files and directories. If this privilege is held, the READ\_CONTROL, ACCESS\_SYSTEM\_SECURITY, FILE\_GENERIC\_READ, and FILE\_TRAVERSE rights are granted. |
| sechangenotifyprivilege | oval-def:  EntityStateBoolType | 0..1 | false | Gives the user the privilege to bypass traverse checking. This privilege is enabled by default for all users. |
| secreateglobalprivilege | oval-def:  EntityStateBoolType | 0..1 | false | Gives the user the privilege to create global objects. It is enabled by default for administrators, services, and the local system account. |
| secreatepagefileprivilege | oval-def:  EntityStateBoolType | 0..1 | false | Gives the user the privilege to create a pagefile. |
| secreatepermanentprivilege | oval-def:  EntityStateBoolType | 0..1 | false | Gives the user the privilege to create permanent shared object. |
| secreatesymboliclinkprivilege | oval-def:  EntityStateBoolType | 0..1 | false | Gives the user the privilege to create symbolic links. |
| secreatetokenprivilege | oval-def:  EntityStateBoolType | 0..1 | false | Gives the user the privilege to create a token object. |
| sedebugprivilege | oval-def:  EntityStateBoolType | 0..1 | false | Gives the user the privilege to debug programs, especially to debug and adjust the memory of a process owned by another account. |
| seenabledelegationprivilege | oval-def:  EntityStateBoolType | 0..1 | false | Gives the user the privilege to enable computer and user accounts to be trusted for delegation. |
| seimpersonateprivilege | oval-def:  EntityStateBoolType | 0..1 | false | Gives the user the privilege to impersonate a client after authentication. |
| seincreasebasepriorityprivilege | oval-def:  EntityStateBoolType | 0..1 | false | Gives the user the privilege to increase scheduling priority. |
| seincreasequotaprivilege | oval-def:  EntityStateBoolType | 0..1 | false | Gives the user the privilege to adjust memory quotas for a process. |
| seincreaseworkingsetprivilege | oval-def:  EntityStateBoolType | 0..1 | false | Gives the user the privilege to increase a process working set. |
| seloaddriverprivilege | oval-def:  EntityStateBoolType | 0..1 | false | Gives the user the privilege to load and unload device drivers. |
| selockmemoryprivilege | oval-def:  EntityStateBoolType | 0..1 | false | Gives the user the privilege to lock pages in memory. |
| semachineaccountprivilege | oval-def:  EntityStateBoolType | 0..1 | false | Gives the user the privilege to add workstations to domain. |
| Semanagevolumeprivilege | oval-def:  EntityStateBoolType | 0..1 | false | Gives the user the privilege to manage the files on a volume. |
| seprofilesingleprocessprivilege | oval-def:  EntityStateBoolType | 0..1 | false | Gives the user the privilege to profile a single process. |
| serelabelprivilege | oval-def:  EntityStateBoolType | 0..1 | false | Gives the user the privilege to modify an object label. |
| seremoteshutdownprivilege | oval-def:  EntityStateBoolType | 0..1 | false | Gives the user the privilege to force shutdown from a remote system. |
| serestoreprivilege | oval-def:  EntityStateBoolType | 0..1 | false | Gives the user the privilege to restore files and directories. The following access rights are granted if this privilege is held: WRITE\_DAC, WRITE\_OWNER, ACCESS\_SYSTEM\_SECURITY, FILE\_GENERIC\_WRITE, FILE\_ADD\_FILE, FILE\_ADD\_SUBDIRECTORY, and DELETE. |
| sesecurityprivilege | oval-def:  EntityStateBoolType | 0..1 | false | Gives the user the privilege to manage auditing and security log. |
| seshutdownprivilege | oval-def:  EntityStateBoolType | 0..1 | false | Gives the user the privilege to shut down the system. |
| sesyncagentprivilege | oval-def:  EntityStateBoolType | 0..1 | false | Gives the user the privilege to synchronize directory service data. This privilege enables the holder to read all objects and properties in the directory, regardless of the protection on the objects and properties.  By default, it is assigned to the Administrator and LocalSystem accounts on domain controllers. |
| sesystemenvironmentprivilege | oval-def:  EntityStateBoolType | 0..1 | false | Gives the user the privilege to modify firmware environment values, especially to modify the nonvolatile RAM of systems that use this type of memory to store configuration information. |
| sesystemprofileprivilege | oval-def:  EntityStateBoolType | 0..1 | false | Gives the user the privilege to profile system performance. |
| sesystemtimeprivilege | oval-def:  EntityStateBoolType | 0..1 | false | Gives the user the privilege to change the system time. |
| setakeownershipprivilege | oval-def:  EntityStateBoolType | 0..1 | false | Gives the user the privilege to take ownership of files or other objects. It allows the owner value to be set only to those values that the holder may legitimately assign as the owner of an object. |
| setcbprivilege | oval-def:  EntityStateBoolType | 0..1 | false | Gives the user the privilege to act as part of the operating system, i.e. as part of the Trusted Computer Base (TCB).  Some trusted protected subsystems are granted this privilege. |
| setimezoneprivilege | oval-def:  EntityStateBoolType | 0..1 | false | Gives the user the privilege to change the time zone. |
| seundockprivilege | oval-def:  EntityStateBoolType | 0..1 | false | Gives the user the privilege to remove the computer from a docking station. |
| seunsolicitedinputprivilege | oval-def:  EntityStateBoolType | 0..1 | false | Allows the user to read unsolicited input from a terminal device. |
| sebatchlogonright | oval-def:  EntityStateBoolType | 0..1 | false | Grants the right for an account to log on using the batch logon type. |
| seinteractivelogonright | oval-def:  EntityStateBoolType | 0..1 | false | Grants the right for an account to log on using the interactive logon type. |
| senetworklogonright | oval-def:  EntityStateBoolType | 0..1 | false | Grants the right for an account to log on using the network logon type. |
| seremoteinteractivelogonright | oval-def:  EntityStateBoolType | 0..1 | false | Grants the right for an account to log on remotely using the interactive logon type. |
| seservicelogonright | oval-def:  EntityStateBoolType | 0..1 | false | Grants the right for an account to log on using the service logon type. |
| sedenybatchlogonright | oval-def:  EntityStateBoolType | 0..1 | false | Denies the right for an account to log on using the batch logon type. |
| sedenyinteractivelogonright | oval-def:  EntityStateBoolType | 0..1 | false | Denies the right for an account to log on using the interactive logon type. |
| sedenynetworklogonright | oval-def:  EntityStateBoolType | 0..1 | false | Denies the right for an account to log on using the network logon type. |
| sedenyremoteinteractivelogonright | oval-def:  EntityStateBoolType | 0..1 | false | Denies the right for an account to log on remotely using the interactive logon type. |
| sedenyservicelogonright | oval-def:  EntityStateBoolType | 0..1 | false | Denies the right for an account to log on using the service logon type. |
| setrustedcredmanaccessnameright | oval-def:  EntityStateBoolType | 0..1 | false | Gives the user the privilege to access Credential Manager as a trusted caller. NOTE: This is a privilege (referred to as **SE\_TRUSTED\_CREDMAN\_ACCESS\_NAME)**, not a right. |

## win-sc:accesstoken\_item

The accesstoken\_item construct holds information about the individual privileges and rights associated with a specific access token. All attributes ending in "privilege" are considered access token privileges[[192]](#footnote-192), and all attributes ending in "right", with the exception of setrustedcredmanaccessnameright, which is a privilege[[193]](#footnote-193), are access token rights[[194]](#footnote-194).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| security\_principle | oval-sc:  EntityItemStringType | 0..1 | false | Identifies an access token to test for. Security principals include users or groups with either local or domain accounts, and computer accounts created when a computer joins a domain.  In Windows, security principals are case-insensitive. As a result, it is recommended that the case-insensitive operations are used for this entity. |
| seassignprimarytokenprivilege | oval-sc:EntityItemBoolType | 0..1 | false | Gives the user the privilege to replace a process-level token. |
| seauditprivilege | oval-sc:EntityItemBoolType | 0..1 | false | Gives the user the privilege to generate security audits. |
| sebackupprivilege | oval-sc:EntityItemBoolType | 0..1 | false | Gives the user the privilege to back up files and directories. If this privilege is held, the READ\_CONTROL, ACCESS\_SYSTEM\_SECURITY, FILE\_GENERIC\_READ, and FILE\_TRAVERSE rights are granted. |
| sechangenotifyprivilege | oval-sc:EntityItemBoolType | 0..1 | false | Gives the user the privilege to bypass traverse checking. This privilege is enabled by default for all users. |
| secreateglobalprivilege | oval-sc:EntityItemBoolType | 0..1 | false | Gives the user the privilege to create global objects. It is enabled by default for administrators, services, and the local system account. |
| secreatepagefileprivilege | oval-sc:EntityItemBoolType | 0..1 | false | Gives the user the privilege to create a pagefile. |
| secreatepermanentprivilege | oval-sc:EntityItemBoolType | 0..1 | false | Gives the user the privilege to create permanent shared object. |
| secreatesymboliclinkprivilege | oval-sc:EntityItemBoolType | 0..1 | false | Gives the user the privilege to create symbolic links. |
| secreatetokenprivilege | oval-sc:EntityItemBoolType | 0..1 | false | Gives the user the privilege to create a token object. |
| sedebugprivilege | oval-sc:EntityItemBoolType | 0..1 | false | Gives the user the privilege to debug programs, especially to debug and adjust the memory of a process owned by another account. |
| seenabledelegationprivilege | oval-sc:EntityItemBoolType | 0..1 | false | Gives the user the privilege to enable computer and user accounts to be trusted for delegation. |
| seimpersonateprivilege | oval-sc:EntityItemBoolType | 0..1 | false | Gives the user the privilege to impersonate a client after authentication. |
| seincreasebasepriorityprivilege | oval-sc:EntityItemBoolType | 0..1 | false | Gives the user the privilege to increase scheduling priority. |
| seincreasequotaprivilege | oval-sc:EntityItemBoolType | 0..1 | false | Gives the user the privilege to adjust memory quotas for a process. |
| seincreaseworkingsetprivilege | oval-sc:EntityItemBoolType | 0..1 | false | Gives the user the privilege to increase a process working set. |
| Seloaddriverprivilege | oval-sc:EntityItemBoolType | 0..1 | false | Gives the user the privilege to load and unload device drivers. |
| selockmemoryprivilege | oval-sc:EntityItemBoolType | 0..1 | false | Gives the user the privilege to lock pages in memory. |
| semachineaccountprivilege | oval-sc:EntityItemBoolType | 0..1 | false | Gives the user the privilege to add workstations to domain. |
| semanagevolumeprivilege | oval-sc:EntityItemBoolType | 0..1 | false | Gives the user the privilege to manage the files on a volume. |
| seprofilesingleprocessprivilege | oval-sc:EntityItemBoolType | 0..1 | false | Gives the user the privilege to profile a single process. |
| serelabelprivilege | oval-sc:EntityItemBoolType | 0..1 | false | Gives the user the privilege to modify an object label. |
| seremoteshutdownprivilege | oval-sc:EntityItemBoolType | 0..1 | false | Gives the user the privilege to force shutdown from a remote system. |
| serestoreprivilege | oval-sc:EntityItemBoolType | 0..1 | false | Gives the user the privilege to restore files and directories. The following access rights are granted if this privilege is held: WRITE\_DAC, WRITE\_OWNER, ACCESS\_SYSTEM\_SECURITY, FILE\_GENERIC\_WRITE, FILE\_ADD\_FILE, FILE\_ADD\_SUBDIRECTORY, and DELETE. |
| sesecurityprivilege | oval-sc:EntityItemBoolType | 0..1 | false | Gives the user the privilege to manage auditing and security log. |
| seshutdownprivilege | oval-sc:EntityItemBoolType | 0..1 | false | Gives the user the privilege to shut down the system. |
| sesyncagentprivilege | oval-sc:EntityItemBoolType | 0..1 | false | Gives the user the privilege to synchronize directory service data. This privilege enables the holder to read all objects and properties in the directory, **regardless** of the protection on the objects and properties.  By default, it is assigned to the Administrator and LocalSystem accounts on domain controllers. |
| sesystemenvironmentprivilege | oval-sc:EntityItemBoolType | 0..1 | false | Gives the user the privilege to modify firmware environment values, especially to modify the nonvolatile RAM of systems that use this type of memory to store configuration information. |
| sesystemprofileprivilege | oval-sc:EntityItemBoolType | 0..1 | false | Gives the user the privilege to profile system performance. |
| sesystemtimeprivilege | oval-sc:EntityItemBoolType | 0..1 | false | Gives the user the privilege to change the system time. |
| setakeownershipprivilege | oval-sc:EntityItemBoolType | 0..1 | false | Gives the user the privilege to take ownership of files or other objects. It allows the owner value to be set **only** to those values that the holder may legitimately assign as the owner of an object. |
| setcbprivilege | oval-sc:EntityItemBoolType | 0..1 | false | Gives the user the privilege to act as part of the operating system, i.e. as part of the Trusted Computer Base (TCB). Some trusted protected subsystems are granted this privilege. |
| setimezoneprivilege | oval-sc:EntityItemBoolType | 0..1 | false | Gives the user the privilege to change the time zone. |
| seundockprivilege | oval-sc:EntityItemBoolType | 0..1 | false | Gives the user the privilege to remove the computer from a docking station. |
| seunsolicitedinputprivilege | oval-sc:EntityItemBoolType | 0..1 | false | Allows the user to read unsolicited input from a terminal device. |
| sebatchlogonright | oval-sc:EntityItemBoolType | 0..1 | false | Grants the right for an account to log on using the batch logon type. |
| seinteractivelogonright | oval-sc:EntityItemBoolType | 0..1 | false | Grants the right for an account to log on using the interactive logon type. |
| senetworklogonright | oval-sc:EntityItemBoolType | 0..1 | false | Grants the right for an account to log on using the network logon type. |
| seremoteinteractivelogonright | oval-sc:EntityItemBoolType | 0..1 | false | Grants the right for an account to log on remotely using the interactive logon type. |
| seservicelogonright | oval-sc:EntityItemBoolType | 0..1 | false | Grants the right for an account to log on using the service logon type. |
| sedenybatchLogonright | oval-sc:EntityItemBoolType | 0..1 | false | Denies the right for an account to log on using the batch logon type. |
| sedenyinteractivelogonright | oval-sc:EntityItemBoolType | 0..1 | false | Denies the right for an account to log on using the interactive logon type. |
| sedenynetworklogonright | oval-sc:EntityItemBoolType | 0..1 | false | Denies the right for an account to log on using the network logon type. |
| sedenyremoteInteractivelogonright | oval-sc:EntityItemBoolType | 0..1 | false | Denies the right for an account to log on remotely using the interactive logon type. |
| sedenyservicelogonright | oval-sc:EntityItemBoolType | 0..1 | false | Denies the right for an account to log on using the service logon type. |
| setrustedcredmanaccessnameright | oval-sc:EntityItemBoolType | 0..1 | false | Gives the user the privilege to access Credential Manager as a trusted caller. NOTE: This is a privilege (referred to as **SE\_TRUSTED\_CREDMAN\_ACCESS\_NAME)**, not a right. |

## win-def:auditeventpolicy\_test

The auditeventpolicy\_test is used to make assertions about the different types of events the system should audit[[195]](#footnote-195). The auditeventpolicy\_test MUST reference one auditeventpolicy\_object and zero or more auditeventpolicy\_states.  


### Known Supported Platforms

* Windows XP
* Windows Vista
* Windows 7

## win-def:auditeventpolicy\_object

The auditeventpolicy\_object construct defines the set of audit events whose associated information should be collected and represented as auditeventpolicy\_items. Because there is only one object relating to audit event policy (the system as a whole), there are no child entities defined for this object, so it is considered empty.



## win-def:auditeventpolicy\_state

The auditeventpolicy\_state construct is used by a auditeventpolicy\_test to specify the different system activities that can be associated with a given auditeventpolicy\_object under Microsoft Windows platforms. The entities correspond to constants under the POLICY\_AUDIT\_EVENT\_TYPE enumeration which all start with "AuditCategory"[[196]](#footnote-196).



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| account\_logon | win-def:  EntityStateAuditType | 0..1 | false | The OS MUST audit each instance of a user attempt to log on or log off this computer, as well as audit logon attempts by privileged accounts that log on to the domain controller. |
| account\_management | win-def:  EntityStateAuditType | 0..1 | false | The OS MUST audit attempts to create, delete, or change user or group accounts, as well as perform password changes. |
| detailed\_tracking | win-def:  EntityStateAuditType | 0..1 | false | The OS MUST audit specific events, such as program activation, some forms of handle duplication, indirect access to an object, and process exit. |
| directory\_service\_access | win-def:  EntityStateAuditType | 0..1 | false | The OS MUST audit attempts to access the directory service. |
| logon | win-def:EntityStateAuditType | 0..1 | false | The OS MUST audit each time this computer validates the credentials of an account. |
| object\_access | win-def:  EntityStateAuditType | 0..1 | false | The OS MUST audit each instance of user attempts to access a non-Active Directory object, such as a file, that has its own system access control (SACL) specified.  The type of access request, such as Write, Read, or Modify, and the account making the request MUST match the settings in the SACL. |
| policy\_change | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit attempts to change Policy object rules, such as user rights assignment policy, audit policy, account policy, or trust policy. |
| privilege\_use | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit each instance of user attempts to use privileges. |
| system | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit attempts to change the system time, startup, restart, or shutdown the system, and load extensible authentication features.  Also, it should audit the loss of audited events due to auditing system failure and any instance of a security log size that exceeds a configurable warning threshold level. |

## win-sc:auditeventpolicy\_\_item

The auditeventpolicy\_item construct stores the different types of events the system should audit. The attributes in the spec correspond to constants under the POLICY\_AUDIT\_EVENT\_TYPE enumeration which all start with "AuditCategory"[[197]](#footnote-197).



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| account\_logon | win-def:  EntityItemAuditType | 0..1 | false | The OS MUST audit each instance of a user attempt to log on or log off this computer, as well as audit logon attempts by privileged accounts that log on to the domain controller. |
| account\_management | win-def:  EntityItemAuditType | 0..1 | false | The OS MUST audit attempts to create, delete, or change user or group accounts, as well as perform password changes. |
| detailed\_tracking | win-def:  EntityItemAuditType | 0..1 | false | The OS MUST audit specific events, such as program activation, some forms of handle duplication, indirect access to an object, and process exit. |
| directory\_service\_access | win-def:  EntityItemAuditType | 0..1 | false | The OS MUST audit attempts to access the directory service. |
| logon | win-def:  EntityItemAuditType | 0..1 | false | The OS MUST audit each time this computer validates the credentials of an account. |
| object\_access | win-def:  EntityItemAuditType | 0..1 | false | The OS MUST audit each instance of user attempts to access a non-Active Directory object, such as a file, that has its own system access control (SACL) specified.  The type of access request, such as Write, Read, or Modify, and the account making the request MUST match the settings in the SACL. |
| policy\_change | win-def:  EntityItemAuditType | 0..1 | false | The OS must audit attempts to change Policy object rules, such as user rights assignment policy, audit policy, account policy, or trust policy. |
| privilege\_use | win-def:  EntityItemAuditType | 0..1 | false | The OS must audit each instance of user attempts to use privileges. |
| system | win-def:  EntityItemAuditType | 0..1 | false | The OS must audit attempts to change the system time, startup, restart, or shutdown the system, and load extensible authentication features.  Also, it should audit the loss of audited events due to auditing system failure and any instance of a security log size that exceeds a configurable warning threshold level. |

## win-def:EntityStateAuditType

The EntityStateAuditType restricts a string value to a specific set of values that describe which audit records should be generated: AUDIT\_FAILURE, AUDIT\_NONE, AUDIT\_SUCCESS, and AUDIT\_SUCCESS\_FAILURE. These values describe the possible hives in the registry.

|  |  |
| --- | --- |
| Enumeration Value | Description |
| AUDIT\_FAILURE | This value indicates that audits must be performed on ALL UNSUCCESSFUL occurrences of specified events when auditing is enabled. |
| AUDIT\_NONE | This value indicates that auditing options must be cancelled for the specified events. |
| AUDIT\_SUCCESS | This value indicates that audits must be performed on ALL SUCCESSFUL occurrences of specified events when auditing is enabled. |
| AUDIT\_SUCCESS\_FAILURE | This value indicates that audits must be performed on ALL SUCCESSFUL AND UNSUCCESSFUL occurrences of specified events when auditing is enabled. |
| *<empty string>* | This value indicates that no value has been specified and is permitted here to allow for an empty entity which is associated with a reference to an OVAL Variable. |

## win-sc:EntityItemAuditType

The EntityItemAuditType restricts a string value to a specific set of values that describe which audit records should be generated: AUDIT\_FAILURE, AUDIT\_NONE, AUDIT\_SUCCESS, and AUDIT\_SUCCESS\_FAILURE. These values describe the possible hives in the registry.

|  |  |
| --- | --- |
| Enumeration Value | Description |
| AUDIT\_FAILURE | This value indicates that audits must be performed on ALL UNSUCCESSFUL occurrences of specified events when auditing is enabled. |
| AUDIT\_NONE | This value indicates that auditing options must be cancelled for the specified events. |
| AUDIT\_SUCCESS | This value indicates that audits must be performed on ALL SUCCESSFUL occurrences of specified events when auditing is enabled. |
| AUDIT\_SUCCESS\_FAILURE | This value indicates that audits must be performed on ALL SUCCESSFUL AND UNSUCCESSFUL occurrences of specified events when auditing is enabled. |
| *<empty string>* | This value indicates that no value has been specified and is permitted here to allow for an empty entity which is associated with a reference to an OVAL Variable. |

## win-def:auditeventpolicysubcategories\_test

The auditeventpolicysubcategories\_test is used to make assertions about the different audit event policy settings on a Windows system[[198]](#footnote-198). The auditeventpolicysubcategories\_test MUST reference one auditeventpolicysubcategories\_object and zero or more auditeventpolicysubcategories\_states.  


### Known Supported Platforms

* Windows XP
* Windows Vista
* Windows 7 (not guaranteed for the kerberos\_ticket\_events category)

## win-def:auditeventpolicysubcategories\_object

The auditeventpolicysubcategories\_object construct defines the set of audit event policy subcategories whose associated information should be collected and represented as auditeventpolicysubcategories\_items. Because there is only one object relating to audit event policy subcategories (the system as a whole), there are no child entities defined for this object, so it is considered empty.



## win-def: auditeventpolicysubcategories\_state

The auditeventpolicysubcategories\_state construct is used by a auditeventpolicysubcategories\_test to specify the different system activities that can be associated with a given auditeventpolicysubcategories\_object under Microsoft Windows platforms[[199]](#footnote-199).



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| credential\_validation | win-def:  EntityStateAuditType | 0..1 | false | The OS MUST audit events that are generated by validation tests on user account logon credentials. This has GUID {0CCE923F-69AE-11D9-BED3-505054503030}. |
| kerberos\_authentication\_service | win-def:  EntityStateAuditType | 0..1 | false | The OS MUST audit events that are generated by Kerberos authentication ticket-granting ticket (TGT) requests. This has GUID {0CCE9242-69AE-11D9-BED3-505054503030}. |
| kerberos\_service\_ticket\_operations | win-def:  EntityStateAuditType | 0..1 | false | The OS MUST audit events that are generated by Kerberos service ticket requests. This has GUID {0CCE9240-69AE-11D9-BED3-505054503030}. |
| kerberos\_ticket\_events | win-def:  EntityStateAuditType | 0..1 | false | The OS MUST audit events that involve validation tests on Kerberos tickets submitted for a user account logon request.[[200]](#footnote-200) |
| other\_account\_logon\_events | win-def:  EntityStateAuditType | 0..1 | false | The OS MUST audit events generated by responses to credential requests submitted for a user account logon that are not credential validation or Kerberos tickets. This has GUID {0CCE9241-69AE-11D9-BED3-505054503030}. |
| application\_group\_management | win-def:  EntityStateAuditType | 0..1 | false | The OS MUST audit events generated by changes to application groups. This has GUID {0CCE9239-69AE-11D9-BED3-505054503030}. |
| computer\_account\_management | win-def:  EntityStateAuditType | 0..1 | false | The OS MUST audit events generated by changes to computer accounts, such as when a computer account is created, changed, or deleted. This has GUID {0CCE9236-69AE-11D9-BED3-505054503030}. |
| distribution\_group\_management | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit events generated by changes to distribution groups. This has GUID {0CCE9238-69AE-11D9-BED3-505054503030}. |
| other\_account\_management\_events | win-def:  EntityStateAuditType | 0..1 | false | The OS MUST audit events generated by other user account changes that are not covered in the account management category, i.e. changes other than those related to user account, computer account, security group, distribution group, and application group management. This has GUID {0CCE923A-69AE-11D9-BED3-505054503030}. |
| security\_group\_management | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit events generated by changes to security groups. This has GUID {0CCE9237-69AE-11D9-BED3-505054503030}. |
| user\_account\_management | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit events generated by changes to user accounts. This has GUID {0CCE9235-69AE-11D9-BED3-505054503030}. |
| dpapi\_activity | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit events generated when encryption or decryption requests are made to the Data Protection application interface (DPAPI). DPAPI is used to protect secret information such as stored password and key information. This has GUID {0CCE922D-69AE-11D9-BED3-505054503030} |
| process\_creation | win-def:  EntityStateAuditType | 0..1 | false | This subcategory audits events generated when a process is created or starts. The name of the application or user that created the process is also audited. This has GUID {0CCE922B-69AE-11D9-BED3-505054503030}. |
| process\_termination | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit events generated  when a process ends. This has GUID {0CCE922C-69AE-11D9-BED3-505054503030}. |
| rpc\_events | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit events generated by inbound remote procedure call (RPC) connections. This has GUID {0CCE922E-69AE-11D9-BED3-505054503030}. |
| directory\_service\_access | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit events generated when an AD DS object is accessed. This has GUID {0CCE923B-69AE-11D9-BED3-505054503030}. |
| directory\_service\_changes | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit events  generated by changes to AD DS objects. Events are logged when an object is created, deleted, modified, moved, or undeleted. This has GUID {0CCE923C-69AE-11D9-BED3-505054503030}. |
| directory\_service\_replication | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit events generated by replication between two AD DS domain controllers. This has GUID {0CCE923D-69AE-11D9-BED3-505054503030}. |
| detailed\_directory\_service\_replication | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit events generated by detailed AD DS[[201]](#footnote-201) replication between domain controllers. This has GUID {0CCE923E-69AE-11D9-BED3-505054503030}. |
| account\_lockout | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit events generated by a failed attempt to log on to an account that is locked out. This has GUID {0CCE9217-69AE-11D9-BED3-505054503030}. |
| ipsec\_extended\_mode | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit events generated by Internet Key Exchange protocol (IKE) and Authenticated Internet Protocol (AuthIP) during Extended Mode negotiations. This has GUID {0CCE921A-69AE-11D9-BED3-505054503030}. |
| ipsec\_main\_mode | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit events generated by Internet Key Exchange protocol (IKE) and Authenticated Internet Protocol (AuthIP) during Main Mode negotiations. This has GUID {0CCE9218-69AE-11D9-BED3-505054503030}. |
| ipsec\_quick\_mode | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit events generated by Internet Key Exchange protocol (IKE) and Authenticated Internet Protocol (AuthIP) during Quick Mode negotiations. This has GUID {0CCE9219-69AE-11D9-BED3-505054503030}. |
| logoff | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit events generated by closing a logon session. These events occur on the computer that was accessed. For an interactive logon, the security audit event is generated on the computer that the user account logged on to. This has GUID {0CCE9216-69AE-11D9-BED3-505054503030}. |
| logon | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit events generated by user account logon attempts on a computer. This has GUID {0CCE9215-69AE-11D9-BED3-505054503030}. |
| network\_policy\_server | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit events generated by RADIUS (IAS) and Network Access Protection (NAP) user access requests. These requests can be Grant, Deny, Discard, Quarantine, Lock, and Unlock. This has GUID {0CCE9243-69AE-11D9-BED3-505054503030}. |
| other\_logon\_logoff\_events | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit events generated by other events related to logon and logoff that are not included in the Logon/Logoff category. This has GUID {0CCE921C-69AE-11D9-BED3-505054503030}. |
| special\_logon | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit events generated by special logons. This has GUID {0CCE921B-69AE-11D9-BED3-505054503030}. |
| application\_generated | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit applications that generate events by using the Windows Auditing application programming interfaces (APIs). Applications designed to use the Windows Auditing API use this subcategory to log auditing events related to their function. This has GUID {0CCE9222-69AE-11D9-BED3-505054503030}. |
| certification\_services | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit Active Directory Certificate Services (AD CS) operations. This has GUID {0CCE9221-69AE-11D9-BED3-505054503030}. |
| detailed\_file\_share | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit every attempt to access objects in a shared folder. This has GUID {0CCE9244-69AE-11D9-BED3-505054503030}. |
| file\_share | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit attempts to access a shared folder. This has GUID {0CCE9224-69AE-11D9-BED3-505054503030}. |
| file\_system | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit attempts to access file system objects. A security audit event is generated only for objects that have SACLs and only if the type of access requested, such as Write, Read, or Modify, and the account making the request match the settings in the SACL. This has GUID {0CCE921D-69AE-11D9-BED3-505054503030}. |
| filtering\_platform\_connection | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit connections that are allowed or blocked by the Windows Filtering Platform (WFP). This has GUID {0CCE9226-69AE-11D9-BED3-505054503030}. |
| filtering\_platform\_packet\_drop | win-def:  EntityStateAuditType | 0..1 | false | This OS must audit packets that are dropped by the Windows Filtering Platform (WFP). |
| handle\_manipulation | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit events generated when a handle to an object is opened or closed. Only objects with a matching SACL generate security audit events.  Open and close handle events will be audited when both the Handle Manipulation subcategory is enabled along with the corresponding resource manager identified by other Object Access audit subcategory, like File System or Registry.  Enabling Handle Manipulation causes implementation-specific security event data to be logged identifying the permissions that were used to grant or deny the access requested by the user; this is also known as "Reason for access". This has GUID {0CCE9223-69AE-11D9-BED3-505054503030}. |
| kernel\_object | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit attempts to access the system kernel, which include mutexes and semaphores. Only kernel objects with a matching SACL generate security audit events. This has GUID {0CCE921F-69AE-11D9-BED3-505054503030}. |
| other\_object\_access\_events | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit events generated by the management of Task Scheduler jobs or COM+ objects. |
| registry | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit attempts to access registry objects. A security audit event is generated only for objects that have SACLs and only if the type of access requested, such as Read, Write, or Modify, and the account making the request match the settings in the SACL. This has GUID {0CCE921E-69AE-11D9-BED3-505054503030}. |
| sam | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit events generated by attempts to access Security Accounts Manager (SAM) objects. This has GUID {0CCE9220-69AE-11D9-BED3-505054503030}. |
| audit\_policy\_change | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit changes in security audit policy settings. This has GUID {0CCE922F-69AE-11D9-BED3-505054503030}. |
| authentication\_policy\_change | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit events generated by changes to the authentication policy. This has GUID {0CCE9230-69AE-11D9-BED3-505054503030}. |
| authorization\_policy\_change | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit events generated by changes to the authorization policy. This has GUID {0CCE9231-69AE-11D9-BED3-505054503030}. |
| filtering\_platform\_policy\_change | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit events generated by changes to the Windows Filtering Platform (WFP). This has GUID {0CCE9233-69AE-11D9-BED3-505054503030}. |
| mpssvc\_rule\_level\_policy\_change | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit events generated by changes in policy rules used by Windows Firewall. This has GUID {0CCE9232-69AE-11D9-BED3-505054503030}. |
| other\_policy\_change\_events | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit events generated by other security policy changes that are not audited in the Policy Change category. This has GUID {0CCE9234-69AE-11D9-BED3-505054503030}. |
| non\_sensitive\_privilege\_use | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit events generated by the use of nonsensitive privileges  (user rights), such as logging on locally or with a Remote Desktop connection, changing the system time, or removing a computer from a docking station. This has GUID {0CCE9229-69AE-11D9-BED3-505054503030}. |
| other\_privilege\_use\_events | win-def:  EntityStateAuditType | 0..1 | false | The OS must TODO. This has GUID {0CCE922A-69AE-11D9-BED3-505054503030}. |
| sensitive\_privilege\_use | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit events generated by the use of sensitive privileges (user rights), such as acting as part of the operating system, backing up files and directories, impersonating a client computer, or generating security audits. This has GUID {0CCE9228-69AE-11D9-BED3-505054503030}. |
| ipsec\_driver | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit events that are generated by the IPsec filter driver. This has GUID {0CCE9213-69AE-11D9-BED3-505054503030}. |
| other\_system\_events | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit any of the following events:  - Startup and shutdown of the Windows Firewall.  - Security policy processing by the Windows Firewall.  - Cryptography key file and migration operations.  This has GUID {0CCE9214-69AE-11D9-BED3-505054503030}. |
| security\_state\_change | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit events generated by changes in the security state of the computer. This has GUID {0CCE9210-69AE-11D9-BED3-505054503030}. |
| security\_system\_extension | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit events related to security system extensions or services. This has GUID {0CCE9211-69AE-11D9-BED3-505054503030}. |
| system\_integrity | win-def:  EntityStateAuditType | 0..1 | false | The OS must audit events that violate the integrity of the security subsystem. This has GUID {0CCE9212-69AE-11D9-BED3-505054503030}. |

## win-sc:auditeventpolicysubcategories\_\_item

The auditeventpolicysubcategories\_item construct stores the different subcategories of event types the system should audit[[202]](#footnote-202).



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| credential\_validation | win-def:EntityItemAuditType | 0..1 | false | The OS MUST audit events that are generated by validation tests on user account logon credentials. This has GUID {0CCE923F-69AE-11D9-BED3-505054503030}. |
| kerberos\_authentication\_service | win-def:EntityItemAuditType | 0..1 | false | The OS MUST audit events that are generated by Kerberos authentication ticket-granting ticket (TGT) requests. This has GUID {0CCE9242-69AE-11D9-BED3-505054503030}. |
| kerberos\_service\_ticket\_operations | win-def:EntityItemAuditType | 0..1 | false | The OS MUST audit events that are generated by Kerberos service ticket requests. This has GUID {0CCE9240-69AE-11D9-BED3-505054503030}. |
| kerberos\_ticket\_events | win-def:EntityItemAuditType | 0..1 | false | The OS MUST audit events that involve validation tests on Kerberos tickets submitted for a user account logon request.[[203]](#footnote-203) |
| other\_account\_logon\_events | win-def:EntityItemAuditType | 0..1 | false | The OS MUST audit events generated by responses to credential requests submitted for a user account logon that are not credential validation or Kerberos tickets. This has GUID {0CCE9241-69AE-11D9-BED3-505054503030}. |
| application\_group\_management | win-def:EntityItemAuditType | 0..1 | false | The OS MUST audit events generated by changes to application groups. This has GUID {0CCE9239-69AE-11D9-BED3-505054503030}. |
| computer\_account\_management | win-def:EntityItemAuditType | 0..1 | false | The OS MUST audit events generated by changes to computer accounts, such as when a computer account is created, changed, or deleted. This has GUID {0CCE9236-69AE-11D9-BED3-505054503030}. |
| distribution\_group\_management | win-def:EntityItemAuditType | 0..1 | false | The OS must audit events generated by changes to distribution groups. This has GUID {0CCE9238-69AE-11D9-BED3-505054503030}. |
| other\_account\_management\_events | win-def:EntityItemAuditType | 0..1 | false | The OS MUST audit events generated by other user account changes that are not covered in the account management category, i.e. changes other than those related to user account, computer account, security group, distribution group, and application group management. This has GUID {0CCE923A-69AE-11D9-BED3-505054503030}. |
| security\_group\_management | win-def:EntityItemAuditType | 0..1 | false | The OS must audit events generated by changes to security groups. This has GUID {0CCE9237-69AE-11D9-BED3-505054503030}. |
| user\_account\_management | win-def:EntityItemAuditType | 0..1 | false | The OS must audit events generated by changes to user accounts. This has GUID {0CCE9235-69AE-11D9-BED3-505054503030}. |
| dpapi\_activity | win-def:EntityItemAuditType | 0..1 | false | The OS must audit events generated when encryption or decryption requests are made to the Data Protection application interface (DPAPI). DPAPI is used to protect secret information such as stored password and key information. This has GUID {0CCE922D-69AE-11D9-BED3-505054503030} |
| process\_creation | win-def:EntityItemAuditType | 0..1 | false | This subcategory audits events generated when a process is created or starts. The name of the application or user that created the process is also audited. This has GUID {0CCE922B-69AE-11D9-BED3-505054503030}. |
| process\_termination | win-def:EntityItemAuditType | 0..1 | false | The OS must audit events generated  when a process ends. This has GUID {0CCE922C-69AE-11D9-BED3-505054503030}. |
| rpc\_events | win-def:EntityItemAuditType | 0..1 | false | The OS must audit events generated by inbound remote procedure call (RPC) connections. This has GUID {0CCE922E-69AE-11D9-BED3-505054503030}. |
| directory\_service\_access | win-def:EntityItemAuditType | 0..1 | false | The OS must audit events generated when an AD DS object is accessed. This has GUID {0CCE923B-69AE-11D9-BED3-505054503030}. |
| directory\_service\_changes | win-def:EntityItemAuditType | 0..1 | false | The OS must audit events  generated by changes to AD DS objects. Events are logged when an object is created, deleted, modified, moved, or undeleted. This has GUID {0CCE923C-69AE-11D9-BED3-505054503030}. |
| directory\_service\_replication | win-def:EntityItemAuditType | 0..1 | false | The OS must audit events generated by replication between two AD DS domain controllers. This has GUID {0CCE923D-69AE-11D9-BED3-505054503030}. |
| detailed\_directory\_service\_replication | win-def:EntityItemAuditType | 0..1 | false | The OS must audit events generated by detailed AD DS[[204]](#footnote-204) replication between domain controllers. This has GUID {0CCE923E-69AE-11D9-BED3-505054503030}. |
| account\_lockout | win-def:EntityItemAuditType | 0..1 | false | The OS must audit events generated by a failed attempt to log on to an account that is locked out. This has GUID {0CCE9217-69AE-11D9-BED3-505054503030}. |
| ipsec\_extended\_mode | win-def:EntityItemAuditType | 0..1 | false | The OS must audit events generated by Internet Key Exchange protocol (IKE) and Authenticated Internet Protocol (AuthIP) during Extended Mode negotiations. This has GUID {0CCE921A-69AE-11D9-BED3-505054503030}. |
| ipsec\_main\_mode | win-def:EntityItemAuditType | 0..1 | false | The OS must audit events generated by Internet Key Exchange protocol (IKE) and Authenticated Internet Protocol (AuthIP) during Main Mode negotiations. This has GUID {0CCE9218-69AE-11D9-BED3-505054503030}. |
| ipsec\_quick\_mode | win-def:EntityItemAuditType | 0..1 | false | The OS must audit events generated by Internet Key Exchange protocol (IKE) and Authenticated Internet Protocol (AuthIP) during Quick Mode negotiations. This has GUID {0CCE9219-69AE-11D9-BED3-505054503030}. |
| logoff | win-def:EntityItemAuditType | 0..1 | false | The OS must audit events generated  by closing a logon session. These events occur on the computer that was accessed. For an interactive logon, the security audit event is generated on the computer that the user account logged on to. This has GUID {0CCE9216-69AE-11D9-BED3-505054503030}. |
| logon | win-def:EntityItemAuditType | 0..1 | false | The OS must audit events generated by user account logon attempts on a computer. This has GUID {0CCE9215-69AE-11D9-BED3-505054503030}. |
| network\_policy\_server | win-def:EntityItemAuditType | 0..1 | false | The OS must audit events generated by RADIUS (IAS) and Network Access Protection (NAP) user access requests. These requests can be Grant, Deny, Discard, Quarantine, Lock, and Unlock. This has GUID {0CCE9243-69AE-11D9-BED3-505054503030}. |
| other\_logon\_logoff\_events | win-def:EntityItemAuditType | 0..1 | false | The OS must audit events generated by other events related to logon and logoff that are not included in the Logon/Logoff category. This has GUID {0CCE921C-69AE-11D9-BED3-505054503030}. |
| special\_logon | win-def:EntityItemAuditType | 0..1 | false | The OS must audit events generated by special logons. This has GUID {0CCE921B-69AE-11D9-BED3-505054503030}. |
| application\_generated | win-def:EntityItemAuditType | 0..1 | false | The OS must audit applications that generate events by using the Windows Auditing application programming interfaces (APIs).  Applications designed to use the Windows Auditing API use this subcategory to log auditing events related to their function. This has GUID {0CCE9222-69AE-11D9-BED3-505054503030}. |
| certification\_services | win-def:EntityItemAuditType | 0..1 | false | The OS must audit Active Directory Certificate Services (AD CS) operations. This has GUID {0CCE9221-69AE-11D9-BED3-505054503030}. |
| detailed\_file\_share | win-def:EntityItemAuditType | 0..1 | false | The OS must audit every attempt to access objects in a shared folder. This has GUID {0CCE9244-69AE-11D9-BED3-505054503030}. |
| file\_share | win-def:EntityItemAuditType | 0..1 | false | The OS must audit attempts to access a shared folder. This has GUID {0CCE9224-69AE-11D9-BED3-505054503030}. |
| file\_system | win-def:EntityItemAuditType | 0..1 | false | The OS must audit attempts to access file system objects. A security audit event is generated only for objects that have SACLs and only if the type of access requested, such as Write, Read, or Modify, and the account making the request match the settings in the SACL. This has GUID {0CCE921D-69AE-11D9-BED3-505054503030}. |
| filtering\_platform\_connection | win-def:EntityItemAuditType | 0..1 | false | The OS must audit connections that are allowed or blocked by the Windows Filtering Platform (WFP). This has GUID {0CCE9226-69AE-11D9-BED3-505054503030}. |
| filtering\_platform\_packet\_drop | win-def:EntityItemAuditType | 0..1 | false | This OS must audit packets that are dropped by the Windows Filtering Platform (WFP). |
| handle\_manipulation | win-def:EntityItemAuditType | 0..1 | false | The OS must audit events generated when a handle to an object is opened or closed. Only objects with a matching SACL generate security audit events.  Open and close handle events will be audited when both the Handle Manipulation subcategory is enabled along with the corresponding resource manager identified by other Object Access audit subcategory, like File System or Registry.  Enabling Handle Manipulation causes implementation-specific security event data to be logged identifying the permissions that were used to grant or deny the access requested by the user; this is also known as "Reason for access". This has GUID {0CCE9223-69AE-11D9-BED3-505054503030}. |
| kernel\_object | win-def:EntityItemAuditType | 0..1 | false | The OS must audit attempts to access the system kernel, which include mutexes and semaphores. Only kernel objects with a matching SACL generate security audit events. This has GUID {0CCE921F-69AE-11D9-BED3-505054503030}. |
| other\_object\_access\_events | win-def:EntityItemAuditType | 0..1 | false | The OS must audit events generated by the management of Task Scheduler jobs or COM+ objects. |
| registry | win-def:EntityItemAuditType | 0..1 | false | The OS must audit attempts to access registry objects. A security audit event is generated only for objects that have SACLs and only if the type of access requested, such as Read, Write, or Modify, and the account making the request match the settings in the SACL. This has GUID {0CCE921E-69AE-11D9-BED3-505054503030}. |
| sam | win-def:EntityItemAuditType | 0..1 | false | The OS must audit events generated by attempts to access Security Accounts Manager (SAM) objects. This has GUID {0CCE9220-69AE-11D9-BED3-505054503030}. |
| audit\_policy\_change | win-def:EntityItemAuditType | 0..1 | false | The OS must audit changes in security audit policy settings. This has GUID {0CCE922F-69AE-11D9-BED3-505054503030}. |
| authentication\_policy\_change | win-def:EntityItemAuditType | 0..1 | false | The OS must audit events generated by changes to the authentication policy. This has GUID {0CCE9230-69AE-11D9-BED3-505054503030}. |
| authorization\_policy\_change | win-def:EntityItemAuditType | 0..1 | false | The OS must audit events generated by changes to the authorization policy. This has GUID {0CCE9231-69AE-11D9-BED3-505054503030}. |
| filtering\_platform\_policy\_change | win-def:EntityItemAuditType | 0..1 | false | The OS must audit events generated by changes to the Windows Filtering Platform (WFP). This has GUID {0CCE9233-69AE-11D9-BED3-505054503030}. |
| mpssvc\_rule\_level\_policy\_change | win-def:EntityItemAuditType | 0..1 | false | The OS must audit events generated by changes in policy rules used by Windows Firewall. This has GUID {0CCE9232-69AE-11D9-BED3-505054503030}. |
| other\_policy\_change\_events | win-def:EntityItemAuditType | 0..1 | false | The OS must audit events generated by other security policy changes that are not audited in the Policy Change category. This has GUID {0CCE9234-69AE-11D9-BED3-505054503030}. |
| non\_sensitive\_privilege\_use | win-def:EntityItemAuditType | 0..1 | false | The OS must audit events generated by the use of nonsensitive privileges  (user rights), such as logging on locally or with a Remote Desktop connection, changing the system time, or removing a computer from a docking station. This has GUID {0CCE9229-69AE-11D9-BED3-505054503030}. |
| other\_privilege\_use\_events | win-def:EntityItemAuditType | 0..1 | false | Not used. This has GUID {0CCE922A-69AE-11D9-BED3-505054503030}. |
| sensitive\_privilege\_use | win-def:EntityItemAuditType | 0..1 | false | The OS must audit events generated by the use of sensitive privileges (user rights), such as acting as part of the operating system, backing up files and directories, impersonating a client computer, or generating security audits. This has GUID {0CCE9228-69AE-11D9-BED3-505054503030}. |
| ipsec\_driver | win-def:EntityItemAuditType | 0..1 | false | The OS must audit events that are generated by the IPsec filter driver. This has GUID {0CCE9213-69AE-11D9-BED3-505054503030}. |
| other\_system\_events | win-def:EntityItemAuditType | 0..1 | false | The OS must audit any of the following events:  - Startup and shutdown of the Windows Firewall.  - Security policy processing by the Windows Firewall.  - Cryptography key file and migration operations.  This has GUID {0CCE9214-69AE-11D9-BED3-505054503030}. |
| security\_state\_change | win-def:EntityItemAuditType | 0..1 | false | The OS must audit events generated by changes in the security state of the computer. This has GUID {0CCE9210-69AE-11D9-BED3-505054503030}. |
| security\_system\_extension | win-def:EntityItemAuditType | 0..1 | false | The OS must audit events related to security system extensions or services. This has GUID {0CCE9211-69AE-11D9-BED3-505054503030}. |
| system\_integrity | win-def:EntityItemAuditType | 0..1 | false | The OS must audit events that violate the integrity of the security subsystem. This has GUID {0CCE9212-69AE-11D9-BED3-505054503030}. |

## win-def:EntityStateAuditType

The EntityStateAuditType restricts a string value to a specific set of values that describe which audit records should be generated: AUDIT\_FAILURE, AUDIT\_NONE, AUDIT\_SUCCESS, and AUDIT\_SUCCESS\_FAILURE. These values describe the possible hives in the registry.

|  |  |
| --- | --- |
| Enumeration Value | Description |
| AUDIT\_FAILURE | This value indicates that audits must be performed on ALL UNSUCCESSFUL occurrences of specified events when auditing is enabled. |
| AUDIT\_NONE | This value indicates that auditing options must be cancelled for the specified events. |
| AUDIT\_SUCCESS | This value indicates that audits must be performed on ALL SUCCESSFUL occurrences of specified events when auditing is enabled. |
| AUDIT\_SUCCESS\_FAILURE | This value indicates that audits must be performed on ALL SUCCESSFUL AND UNSUCCESSFUL occurrences of specified events when auditing is enabled. |
| *<empty string>* | This value indicates that no value has been specified and is permitted here to allow for an empty entity which is associated with a reference to an OVAL Variable. |

## win-sc:EntityItemAuditType

The EntityItemAuditType restricts a string value to a specific set of values that describe which audit records should be generated: AUDIT\_FAILURE, AUDIT\_NONE, AUDIT\_SUCCESS, and AUDIT\_SUCCESS\_FAILURE. These values describe the possible hives in the registry.

|  |  |
| --- | --- |
| Enumeration Value | Description |
| AUDIT\_FAILURE | This value indicates that audits must be performed on ALL UNSUCCESSFUL occurrences of specified events when auditing is enabled. |
| AUDIT\_NONE | This value indicates that auditing options must be cancelled for the specified events. |
| AUDIT\_SUCCESS | This value indicates that audits must be performed on ALL SUCCESSFUL occurrences of specified events when auditing is enabled. |
| AUDIT\_SUCCESS\_FAILURE | This value indicates that audits must be performed on ALL SUCCESSFUL AND UNSUCCESSFUL occurrences of specified events when auditing is enabled. |
| *<empty string>* | This value indicates that no value has been specified and is permitted here to allow for an empty entity which is associated with a reference to an OVAL Variable. |

## win-def:passwordpolicy\_test

The passwordpolicy\_test is used to check specific policies associated with passwords on Windows based systems[[205]](#footnote-205). It is important to note that these policies are specific to certain versions of Windows. Additionally, this information is stored in the SAM or Active Directory and is **encrypted or hidden**, thus the registry\_test and activedirectory57\_test are of NO USE. The passwordpolicy\_test MUST reference one passwordpolicy\_object and zero or more passwordpolicy\_states.  


### Known Supported Platforms

* Windows XP
* Windows Vista
* Windows 7

## win-def:passwordpolicy\_object

The passwordpolicy\_object construct defines the set of policies on Windows passwords whose associated information should be collected and represented as passwordpolicy\_items. Since there is only one object relating to password policy (the system as a whole), there are no child entities defined for this object, so it is considered empty.



## win-def:passwordpolicy\_state

The passwordpolicy\_state construct is used by a passwordpolicy\_test to specify the various policies associated with passwords that can be associated with a given passwordpolicy\_object under Microsoft Windows platforms[[206]](#footnote-206).

In Windows, an administrator can go to the Control Panel, then Administrative Tools, and finally go to Local Security Policy. From there, the alternate names for the policies mentioned correspond to the ones under Account Policies 🡪 Password Policy. NOTE: There can be discrepancies between the different documentations based on the version of Windows running, especially for max\_passwd\_age. Also, times in OVAL are in SECONDS, not DAYS as they are defined in the Windows Control Panel, and TIMEQ\_FOREVER is defined as the value of -1, cast as an unsigned int[[207]](#footnote-207).



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| max\_passwd\_age | oval-def:EntityStateIntType | 0..1 | false | Alternate name: "Maximum password age." Determines the period (**in seconds**) that a password can be used before the system requires the user to change it. In OVAL, values range from 1 \* 86400 (one day) to 999 \* 86400 = 86313600 (999 days) inclusive, where 86400 is the number of seconds in one day.  In addition, max\_passwd\_age can take on the value of TIMEQ\_FOREVER to indicate that passwords NEVER expire. The default in the Default Domain Group Policy Object (GPO), as well as workstations and servers, is 42\*86400 = 3628800 (42 days). |
| min\_passwd\_age | oval-def:EntityStateIntType | 0..1 | false | Alternate name: "Minimum password age." Determines the period (in seconds) that a password must be used before the user can change it.  In OVAL, values range from 0 \* 86400 (changes can happen immediately) to 999 \* 86400 = 86313600 (999 days) inclusive, where 86400 is the number of seconds in one day.  The default in the Default Domain GPO, as well as workstations and servers, is 0. |
| min\_passwd\_len | oval-def:EntityStateIntType | 0..1 | false | Alternate name: "Minimum password length." Determines the least number of characters a user account's password may contain.  In OVAL, values range from 0 to 14 inclusive, where 0 indicates that no password is required. The default in the Default Domain GPO, as well as workstations and servers, is 0. |
| password\_hist\_len | oval-def:EntityStateIntType | 0..1 | false | Alternate name: "Enforce password history." Determines the number of unique new passwords that have to be associated with a user account before an old password can be reused. Values range from 0 to 24 inclusive. The default in the Default Domain GPO, as well as workstations and servers, is 1. |
| password\_complexity | oval-def:  EntityStateBoolType | 0..1 | false | Alternate name: "Password must meet complexity requirements (of the installed password filter)." The part in parenthesis is different depending on the version of Windows in question.  This attribute determines whether passwords meet complexity requirements. The default password filter defined by passfilt.dll (found in Win 2000, but also applies in later versions) requires that a password 1) does not contain all or part of the user's account name, 2) is at least six characters in length, and 3) satisfies three out of the four criteria of containing either uppercase, lowercase, base 10 digits 0-9, and/or nonalphanumeric characters.  Complexity requirements are enforced upon password change or creation. The default in the Default Domain GPO, as well as workstations and servers, is "Disabled," or 0 in OVAL. |
| reversible\_encryption | oval-def:  EntityStateBoolType | 0..1 | false | Alternate name: "Store password using reversible encryption (for all users in the domain)." The part in parenthesis is different depending on the version of Windows in question.  This determines whether Windows will store passwords using reversible encryption.  According to MSDN, storing passwords using reversible encryption is essentially the same as storing clear-text versions of the passwords, so it SHOULD NEVER BE ENABLED unless application requirements outweigh the need to protect password information.  The default in the Default Domain GPO, as well as workstations and servers, is "Disabled," or 0 in OVAL. |

## win-sc:passwordpolicy\_item

The passwordpolicy\_item construct stores the different policies on password that should be collected[[208]](#footnote-208).

In Windows, an administrator can go to the Control Panel, then Administrative Tools, and finally go to Local Security Policy. From there, the alternate names for the policies mentioned correspond to the ones under Account Policies 🡪 Password Policy. NOTE: There can be discrepancies between the different documentations based on the version of Windows running, especially for max\_passwd\_age. Also, times in OVAL are in SECONDS, not DAYS as they are defined in the Windows Control Panel, and TIMEQ\_FOREVER is defined as the value of -1, cast as an unsigned int[[209]](#footnote-209).



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| max\_passwd\_age | oval-def:EntityItemIntType | 0..1 | false | Alternate name: "Maximum password age." Determines the period (in seconds) that a password can be used before the system requires the user to change it.  In OVAL, values range from 1 \* 86400 (one day) to 999 \* 86400 = 86313600 (999 days) inclusive, where 86400 is the number of seconds in one day.  In addition, max\_passwd\_age can take on the value of TIMEQ\_FOREVER to indicate that passwords NEVER expire.  The default in the Default Domain Group Policy Object (GPO), as well as workstations and servers is 42\*86400 = 3628800 (42 days). |
| min\_passwd\_age | oval-def:EntityItemIntType | 0..1 | false | Alternate name: "Minimum password age." Determines the period (in seconds) that a password must be used before the user can change it.  In OVAL, values range from 0 \* 86400 (changes can happen immediately) to 999 \* 86400 = 86313600 (999 days) inclusive, where 86400 is the number of seconds in one day.  The default in the Default Domain GPO, as well as workstations and servers, is 0. |
| min\_passwd\_len | oval-def:EntityItemIntType | 0..1 | false | Alternate name: "Minimum password length." Determines the least number of characters a user account's password may contain.  In OVAL, values range from 0 to 14 inclusive, where 0 indicates that no password is required.  The default in the Default Domain GPO, as well as workstations and servers, is 0. |
| password\_hist\_len | oval-def:EntityItemIntType | 0..1 | false | Alternate name: "Enforce password history." Determines the number of unique new passwords that have to be associated with a user account before an old password can be reused.  Values range from 0 to 24 inclusive. The default in the Default Domain GPO, as well as workstations and servers, is 1. |
| password\_complexity | oval-def:  EntityItemBoolType | 0..1 | false | Alternate name: "Password must meet complexity requirements (of the installed password filter)." The part in parenthesis is different depending on the version of Windows in question.  This attribute determines whether passwords meet complexity requirements.  The default password filter defined by passfilt.dll (found in Win 2000, but also applies in later versions) requires that a password 1) does not contain all or part of the user's account name, 2) is at least six characters in length, and 3) satisfies three out of the four criteria of containing either uppercase, lowercase, base 10 digits 0-9, and/or nonalphanumeric characters.  Complexity requirements are enforced upon password change or creation.  The default in the Default Domain GPO, as well as workstations and servers, is "Disabled," or 0 in OVAL. |
| reversible\_encryption | oval-def:  EntityItemBoolType | 0..1 | false | Alternate name: "Store password using reversible encryption (for all users in the domain)." The part in parenthesis is different depending on the version of Windows in question.  This determines whether Windows will store passwords using reversible encryption.  According to MSDN, storing passwords using reversible encryption is essentially the same as storing clear-text versions of the passwords, so it SHOULD NEVER BE ENABLED unless application requirements outweigh the need to protect password information.  The default in the Default Domain GPO, as well as workstations and servers, is "Disabled," or 0 in OVAL. |

## win-def:lockoutpolicy\_test

The lockoutpolicy\_test is used to make assertions about with lockout information for users and global groups in the security database[[210]](#footnote-210). The lockoutpolicy\_test MUST reference one lockoutpolicy\_object and zero or more lockoutpolicy\_states. 

### Known Supported Platforms

* Windows XP
* Windows Vista
* Windows 7

## win-def:lockoutpolicy\_object

The lockoutpolicy\_object construct defines the applicable lockout information for users and global groups in the security database that should be collected and represented as lockoutpolicy\_items[[211]](#footnote-211). Because there is only one object relating to lockout information (the system as a whole), there are no child entities defined for this object, so it is considered empty.



## win-def: lockoutpolicy\_state

The lockoutpolicy\_state construct is used by a lockoutpolicy\_test to outline the various attributes associated with lockout information for users and global groups in the security database under Microsoft Windows platforms[[212]](#footnote-212). In Windows an administrator can go to the Control Panel and go to Local Security Policy. From there, the policies mentioned are under Account Policies/Account Lockout Policy. When mentioning alternate names for specific attributes, they are referring to the ones in that directory path, except for force\_logoff and lockout\_observation\_window[[213]](#footnote-213). NOTE: There can be discrepancies between the different documentations based on the version of Windows running. Also, times in OVAL are in SECONDS, not MINUTES as they are defined in the Windows Control Panel, and TIMEQ\_FOREVER is defined as the value of -1, cast as an unsigned int[[214]](#footnote-214). 

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| force\_logoff | oval-def:EntityStateIntType | 0..1 | false | Indicates the amount of time in SECONDS (not MINUTES) that an interactive logon session is allowed to continue. |
| lockout\_duration | oval-def:EntityStateIntType | 0..1 | false | Alternate name: "Account lockout duration." Determines the number of SECONDS a locked-out account remains locked out before automatically becoming unlocked.  The available range is from 1 second through 99,999\*60 = 5999940 seconds. If an account lockout threshold is defined, the account lockout duration must be greater than or equal to the reset time.  If you set the account lockout duration to TIMEQ\_FOREVER, the account MUST be locked out until an administrator explicitly unlocks it[[215]](#footnote-215). This policy on has meaning when Account lockout threshold is specified.  The default value is 30 \*60 = 1800 (30 minutes). |
| lockout\_observation\_window | oval-def:EntityStateIntType | 0..1 | false | Indicates the amount of time in SECONDS in which failed password attempts are counted without resetting the count to zero.  This setting can be used to help mitigate lockout issues that are initiated by users. The available range is from 1 second through 99,999\*60 = 5999940 seconds, with a default of 30\*60 = 1800 (30 minutes). |
| lockout\_threshold | oval-def:EntityStateIntType | 0..1 | false | Alternate name: "Account lockout threshold." Determines the number of failed logon attempts that will cause a user account to be locked out.  A locked out account cannot be used until it is reset by an administrator or the account lockout duration has expired.  You can set values between 1 and 999 failed logon attempts, or you can specify that the account will never be locked out by setting the value to 0.  By default, this setting is 0 in the Default Domain Group Policy object (GPO) and in the local security policy of workstations and servers. |

## win-sc: lockoutpolicy \_item

The lockoutpolicy\_item enumerates various attributes associated with lockout information for users and global groups in the security database.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| force\_logoff | oval-def:EntityStateIntType | 0..1 | false | Indicates the amount of time in SECONDS (not MINUTES) that an interactive logon session is allowed to continue. |
| lockout\_duration | oval-def:EntityStateIntType | 0..1 | false | Alternate name: "Account lockout duration." Determines the number of SECONDS a locked-out account remains locked out before automatically becoming unlocked.  The available range is from 1 second through 99,999\*60 = 5999940 seconds. If an account lockout threshold is defined, the account lockout duration must be greater than or equal to the reset time.  If you set the account lockout duration to TIMEQ\_FOREVER, the account MUST be locked out until an administrator explicitly unlocks it[[216]](#footnote-216). This policy on has meaning when Account lockout threshold is specified. The default value is 30 \*60 = 1800 (30 minutes). |
| lockout\_observation\_window | oval-def:EntityStateIntType | 0..1 | false | Indicates the amount of time in SECONDS in which failed password attempts are counted without resetting the count to zero.  This setting can be used to help mitigate lockout issues that are initiated by users. The available range is from 1 second through 99,999\*60 = 5999940 seconds, with a default of 30\*60 = 1800 (30 minutes). |
| lockout\_threshold | oval-def:EntityStateIntType | 0..1 | false | Alternate name: "Account lockout threshold." Determines the number of failed logon attempts that will cause a user account to be locked out.  A locked out account cannot be used until it is reset by an administrator or the account lockout duration has expired. You can set values between 1 and 999 failed logon attempts, or you can specify that the account will never be locked out by setting the value to 0.  By default, this setting is 0 in the Default Domain Group Policy object (GPO) and in the local security policy of workstations and servers. |

## win-def:wmi57\_test

The wmi57\_test is used to make assertions about information accessed by WMI[[217]](#footnote-217). The wmi57\_test MUST reference one wmi57\_object and zero or more wmi57\_states.  


### Known Supported Platforms

* Windows XP
* Windows Vista
* Windows 7

## win-def:wmi57\_object

The wmi57\_object construct defines the applicable WMI information that should be collected and represented as wmi57\_items[[218]](#footnote-218).



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| set | oval-def:set | 0..1 | false | Enables the expression of complex wmi57\_objects that are the result of logically combining and filtering the wmi57\_items that are identified by one or more wmi57\_objects. |
| namespace | oval-def:EntityObjectStringType | 0..1 | false | Specifies which WMI namespace to look under. Each WMI provider normally registers its own WMI namespace and then all its classes within that namespace[[219]](#footnote-219). |
| wql | oval-def:EntityObjectStringType | 0..1 | false | A WQL query used to identify the wmi57\_objects to represent as wmi57\_items. Any valid WQL query is usable with one exception, all fields must be named in the SELECT portion of the query[[220]](#footnote-220). |
| filter | oval-def:filter [2] | 0..\* | false | Allows for the explicit inclusion or exclusion of wmi57\_items from the set of wmi57\_items collected by a wmi57\_object. Please see the OVAL Language Specification [2] for additional information. |

## win-def: wmi57\_state

The wmi57\_state construct is used by a wmi57\_test to outline information to be checked through Microsoft's WMI interface. It specifies the applicable WMI information that can be associated with a given wmi57\_object under Microsoft Windows platforms[[221]](#footnote-221).



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| namespace | oval-def:  EntityStateStringType | 0..1 | false | Specifies which WMI namespace to look under. Each WMI provider normally registers its own WMI namespace and then all its classes within that namespace[[222]](#footnote-222). |
| wql | oval-def:  EntityStateStringType | 0..1 | false | A WQL query used to identify the wmi57\_objects to represent as wmi57\_items. Any valid WQL query is usable with one exception, all fields must be named in the SELECT portion of the query[[223]](#footnote-223). |
| result | oval-def:  EntityStateRecordType | 0..1 | false | The result attribute specifies how to test items in the result set of the specified WQL statement. |

## win-sc:wmi57\_item

The wmi57\_item outlines information to be checked through Microsoft's WMI interface.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| namespace | oval-sc:EntityItemStringType | 0..1 | false | Specifies which WMI namespace to look under. Each WMI provider normally registers its own WMI namespace and then all its classes within that namespace[[224]](#footnote-224). |
| wql | oval-sc:EntityItemStringType | 0..1 | false | A WQL query used to identify the wmi57\_ objects to represent as wmi57\_items. Any valid WQL query is usable with one exception, all fields must be named in the SELECT portion of the query[[225]](#footnote-225). |
| result | oval-sc:  EntityItemRecordType | 0..\* | false | The result attribute specifies how to test items in the result set of the specified WQL statement. |

## win-def:sid\_test

The sid\_test is used to make assertions about the properties associated with the specified trustee[[226]](#footnote-226) name and its corresponding SID[[227]](#footnote-227). If a unique check is needed, use the sid\_sid\_test which matches based on the SID value, which is guaranteed to be unique. The sid\_test MUST reference one sid\_object and zero or more sid\_states.



### Known Supported Platforms

* Windows XP
* Windows Vista
* Windows 7

## win-def:sid\_object

The sid\_object construct defines the object set, in this case a set of SIDs (identified by name), whose associated information should be collected and represented as sid\_items[[228]](#footnote-228).



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| set | oval-def:set | 0..1 | false | Enables the expression of complex sid\_objects that are the result of logically combining and filtering the sid\_items that are identified by one or more sid\_objects. |
| behavior | win-def:SidBehaviors | 0..1 | false | Specifies the behaviors that direct how the sid\_object collects sid\_items from the system. |
| trustee\_name | oval-def:  EntityObjectStringType | 1..1 | false | The trustee\_name attribute is the unique name (case-insensitive in Windows) that is associated to a particular SID.  A SID can be associated with a user, group, or program (such as a Windows service). Because trustee names are case-insensitive, it is recommended that the case-insensitive operations are used for this property[[229]](#footnote-229).  Trustee names in a domain environment SHOULD be identified in the form "domain\trustee name," local trustee names SHOULD be identified in the form "computer name\trustee name," and built-in accounts should be identified by JUST the trustee name without a domain[[230]](#footnote-230). |
| filter | oval-def:filter [2] | 0..\* | false | Allows for the explicit inclusion or exclusion of sid\_items from the set of sid\_items collected by a sid\_object. Please see the OVAL Language Specification [2] for additional information. |

## win-def:SidBehaviors

The SidBehaviors construct defines the behaviors that direct how the sid\_object collects sid\_items from the system. Note that using these behaviors may result in some unique results. For example, a double negative type condition might be created where an object entity says include everything except a specific item, but a behavior is used that might then add that item back in.

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute | Type | Possible Values | Description |
| include\_group | bool | *'true'*  *'false'* | Defines whether or not the group SID should be collected when the trustee\_sid property specifies a group SID.  *'true'*: The group SID MUST be collected when the trustee\_sid property specifies a group SID.  *'false'*: The group SID MUST NOT be collected when the trustee\_sid property specifies a group SID.  **Default Value: true** |
| resolve\_group | bool | *'true'*  *'false'* | Defines whether or not the members of group SIDs should be resolved and collected.  Note that all child groups should also be resolved and any valid domain accounts that are members should also be included.  The intent of this behavior is to end up with a list of all individual users from that system that make up the group once everything has been resolved.  *'true'*: The members of a group SID MUST be resolved and collected.  'false': The members of a group SID MUST NOT be resolved or collected.  **Default Value: false** |

## win-def:sid\_state

The sid\_state construct is used by a sid\_test to specify the different rights that can be associated with a given sid\_object under Microsoft Windows platforms[[231]](#footnote-231).



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| trustee\_name | oval-def:  EntityStateStringType | 0..1 | false | The trustee\_name property is the unique name (case-insensitive in Windows) that is associated to a particular SID.  A SID can be associated with a user, group, or program (such as a Windows service). Because trustee names are case-insensitive, it is recommended that the case-insensitive operations are used for this attribute[[232]](#footnote-232).  Trustee names in a domain environment SHOULD be identified in the form "domain\trustee name," local trustee names SHOULD be identified in the form "computer name\trustee name," and built-in accounts should be identified by JUST the trustee name without a domain[[233]](#footnote-233). |
| trustee\_sid | oval-def:  EntityStateStringType | 0..1 | false | The security identifier (SID) of the specified trustee name. |
| trustee\_domain | oval-def:  EntityStateStringType | 0..1 | false | The domain of the specified trustee name. |

## win-sc:sid\_item

The sid\_item stores the attributes associated with a given sid\_object under Microsoft Windows platforms.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| trustee\_name | oval-sc:EntityItemStringType | 0..1 | false | The trustee\_name property is the unique name (case-insensitive in Windows) that is associated to a particular SID.  A SID can be associated with a user, group, or program (such as a Windows service). Because trustee names are case-insensitive, it is recommended that the case-insensitive operations are used for this attribute[[234]](#footnote-234).  Trustee names in a domain environment SHOULD be identified in the form "domain\trustee name," local trustee names SHOULD be identified in the form "computer name\trustee name," and built-in accounts should be identified by JUST the trustee name without a domain[[235]](#footnote-235). |
| trustee\_sid | oval-sc:EntityItemStringType | 0..1 | false | The security identifier (SID) of the specified trustee name. |
| trustee\_domain | oval-sc:EntityitemStringType | 0..1 | false | The domain of the specified trustee name. |

## win-def:sid\_sid\_test

The sid\_sid\_test is used to check properties associated with the specified SID. Note that this test was added in version 5.4 as a temporary fix. There is a need within the community to identify objects like users and groups by both the name[[236]](#footnote-236) and the SID[[237]](#footnote-237). The sid\_test should be used instead when the object is identified by name. The sid\_sid\_test MUST reference one sid\_sid\_object and zero or more sid\_sid\_states.



### Known Supported Platforms

* Windows XP
* Windows Vista
* Windows 7

## win-def:sid\_sid\_object

The sid\_sid\_object element defines the object set, selected via a designated SID, whose associated information should be collected and represented as sid\_sid\_items.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| set | oval-def:set | 0..1 | false | Enables the expression of complex sid\_sid\_objects that are the result of logically combining and filtering the sid\_sid\_items that are identified by one or more sid\_sid\_objects. |
| behavior | win-def:SidSidBehaviors | 0..1 | false | Specifies the behaviors that direct how the sid\_sid\_object collects sid\_sid\_items from the system. |
| trustee\_sid | oval-def:  EntityObjectStringType | 1..1 | true | The unique SID associated with a user, group, system, or program (such as a Windows service)[[238]](#footnote-238). |
| filter | oval-def:filter [2] | 0..\* | false | Allows for the explicit inclusion or exclusion of sid\_sid\_items from the set of sid\_sid\_items collected by a sid\_sid\_object. Please see the OVAL Language Specification [2] for additional information. |

## win-def:SidSidBehaviors

The SidSidBehaviors construct defines the behaviors that direct how the sid\_sid\_object collects sid\_sid\_items from the system. Note that using these behaviors may result in some unique results. For example, a double negative type condition might be created where an object entity says include everything except a specific item, but a behavior is used that might then add that item back in.

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute | Type | Possible Values | Description |
| include\_group | boolean | *'true'*  *'false'* | Defines whether or not the group SID should be collected when the trustee\_sid property specifies a group SID.  *'true'*: The group SID MUST be collected when the trustee\_sid property specifies a group SID.  *'false'*: The group SID MUST NOT be collected when the trustee\_sid property specifies a group SID.  **Default Value: true** |
| resolve\_group | boolean | *'true'*  *'false'* | Defines whether or not the members of group SIDs should be resolved and collected.  Note that all child groups should also be resolved and any valid domain accounts that are members should also be included.  The intent of this behavior is to end up with a list of all individual users from that system that make up the group once everything has been resolved.  *'true'*: The members of a group SID MUST be resolved and collected.  'false': The members of a group SID MUST NOT be resolved or collected.  **Default Value: false** |

## win-def:sid\_sid\_state

The sid\_sid\_state construct is used by a sid\_sid\_test to specify the attributes associated with a given sid\_sid\_object under Microsoft Windows platforms.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| trustee\_name | oval-def:  EntityStateStringType | 0..1 | false | The trustee\_name property is the unique name (case-insensitive in Windows) that is associated to a particular SID. A SID can be associated with a user, group, or program (such as a Windows service).  Because trustee names are case-insensitive, it is recommended that the case-insensitive operations are used for this property[[239]](#footnote-239).  Trustee names in a domain environment SHOULD be identified in the form "domain\trustee name," local trustee names SHOULD be identified in the form "computer name\trustee name," and built-in accounts should be identified by JUST the trustee name without a domain[[240]](#footnote-240). |
| trustee\_sid | oval-def:  EntityStateStringType | 0..1 | false | The security identifier (SID) of the specified trustee name. |
| trustee\_domain | oval-def:  EntityStateStringType | 0..1 | false | The domain of the specified trustee name. |

## win-sc:sid\_sid\_item

The sid\_sid\_item stores the attributes associated with a given sid\_sid\_object under Microsoft Windows platforms.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| trustee\_name | oval-sc:  EntityItemStringType | 0..1 | false | The trustee\_name property is the unique name (case-insensitive in Windows) that is associated to a particular SID. A SID can be associated with a user, group, or program (such as a Windows service).  Because trustee names are case-insensitive, it is recommended that the case-insensitive operations are used for this property[[241]](#footnote-241).  Trustee names in a domain environment SHOULD be identified in the form "domain\trustee name," local trustee names SHOULD be identified in the form "computer name\trustee name," and built-in accounts should be identified by JUST the trustee name without a domain[[242]](#footnote-242). |
| trustee\_sid | oval-sc:  EntityItemStringType | 0..1 | false | The security identifier (SID) of the specified trustee name. |
| trustee\_domain | oval-sc:  EntityitemStringType | 0..1 | false | The domain of the specified trustee name. |

## win-def:cmdlet\_test

The cmdlet\_test is used to leverage a Powershell cmdlet to check a Windows system. The cmdlet\_test MUST reference one cmdlet\_object and zero or more cmdlet\_states[[243]](#footnote-243).  


### Known Supported Platforms

* Windows XP
* Windows Vista
* Windows 7

## win-def:cmdlet\_object

The cmdlet\_object construct defines the applicable set of cmdlets and parameters that should be collected and represented as cmdlet\_items[[244]](#footnote-244).

In order to ensure the consistency of PowerShell cmdlet support among OVAL interpreters, as well as ensure that the state of a system is not changed, every OVAL interpreter must implement the following requirements. An OVAL interpreter MUST ONLY support the processing of the verbs specified in the EntityObjectCmdletVerbType. If a cmdlet verb that is not defined in this enumeration is discovered, an error SHOULD be reported and the cmdlet MUST NOT be executed on the system. While XML Schema validation will enforce this requirement, it is STRONGLY RECOMMENDED that OVAL interpreters implement a whitelist of allowed cmdlets. This can be done using constrained runspaces which can limit the PowerShell execution environment. For more information, please see Microsoft's documentation on Windows PowerShell Host Application Concepts[[245]](#footnote-245). Certain attributes (such as nouns, verbs, and parameter names) SHOULD align with the MSDN documentation[[246]](#footnote-246).

Furthermore, it is strongly recommended that OVAL interpreters also implement PowerShell support with the NoLanguage mode enabled. The NoLanguage mode ensures that scripts that need to be evaluated are not allowed in the runspace. For more information about the NoLanguage mode, please see Microsoft's documentation on the PSLanguageMode enumeration[[247]](#footnote-247). 

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| set | oval-def:set | 0..1 | false | Enables the expression of complex cmdlet\_objects that are the result of logically combining and filtering the cmdlet\_items that are identified by one or more cmdlet\_objects. |
| module\_name | oval-def:EntityObjectStringType | 1..1 | true | The name of the module that defines the cmdlet[[248]](#footnote-248). When set using the New-Module command in Powershell, the default name is \_\_DynamicModule\_PATHID where "PATHID" is a unique identifier that specifies the path to the dynamic module[[249]](#footnote-249).  If **xsi:nil="true"**, it implies that it does not matter which module name the command comes from. |
| module\_id | win-def:EntityObjectGUIDType | 1..1 | true | A global unique identifier (GUID) instituted so as to avoid module conflict. This is in the form A-B-C-D-E where A is an 8-digit hexadecimal number, B, C, and D are 4-digit hexadecimal numbers, and E is a 12-digit hexadecimal number[[250]](#footnote-250).  If **xsi:nil="true"**, it implies that it does not matter which module GUID the command comes from. |
| module\_version | oval-def:  EntityObjectVersionType | 1..1 | true | Module version in the format of MAJOR.MINOR[[251]](#footnote-251). If **xsi:nil="true"**, it implies that it does not matter which version of the module the command refers to. |
| verb | win-def:  EntityObjectCmdletVerbType | 1..1 | false | The verb name of the cmdlet[[252]](#footnote-252). This verb specifies the action[[253]](#footnote-253) taken by the cmdlet.  NOTE: In Windows Powershell, verbs describe a word that *implies* an action even if that word is not a standard verb in the English language, such as *New*. |
| noun | oval-def:  EntityObjectStringType | 1..1 | false | The noun name of the cmdlet[[254]](#footnote-254). This noun specifies the resource[[255]](#footnote-255) that the cmdlet acts upon. |
| parameters | oval-def:  EntityObjectRecordType | 0..1 | true | The parameters of the cmdlet, that is, the list of properties (name and value pairs) as input to invoke the cmdlet. Each property name must be unique.  If **xsi:nil="true"**, parameters are NOT provided to the cmdlet[[256]](#footnote-256). Also, parameter names SHOULD align with the MSDN documentation[[257]](#footnote-257). |
| select | oval-def:  EntityObjectRecordType | 0..1 | true | A set of name and value pairs used as input to the Select-Object[[258]](#footnote-258) cmdlet in order to target output properties. Each property name MUST be unique.  If **xsi:nil="true"**, these pairs are not provided to the cmdlet. |
| filter | oval-def:filter [2] | 0..\* | false | Allows for the explicit inclusion or exclusion of cmdlet\_items from the set of cmdlet\_items collected by a cmdlet\_object. Please see the OVAL Language Specification [2] for additional information. |

## win-def:cmdlet\_state

The cmdlet\_state construct is used by a cmdlet\_test to make assertions about the presence of PowerShell cmdlet related properties and values obtained from a cmdlet[[259]](#footnote-259). Certain attributes (such as nouns, verbs, and parameter names) SHOULD align with the MSDN documentation[[260]](#footnote-260).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| module\_name | oval-def:EntityStateStringType | 0..1 | false | The name of the module that defines the cmdlet[[261]](#footnote-261). When set using the New-Module command in Powershell, the default name is \_\_DynamicModule\_PATHID where "PATHID" is a unique identifier that specifies the path to the dynamic module[[262]](#footnote-262). |
| module\_id | win-def:EntityStateGUIDType | 0..1 | false | A global unique identifier (GUID) instituted so as to avoid module conflict. This is in the form A-B-C-D-E where A is an 8-digit hexadecimal number, B, C, and D are 4-digit hexadecimal numbers, and E is a 12-digit hexadecimal number[[263]](#footnote-263). |
| module\_version | oval-def:  EntityStateVersionType | 0..1 | false | Module version in the format of MAJOR.MINOR[[264]](#footnote-264). |
| verb | win-def:  EntityStateCmdletVerbType | 0..1 | false | The verb name of the cmdlet[[265]](#footnote-265). This verb specifies the action[[266]](#footnote-266) taken by the cmdlet. NOTE: In Windows Powershell, verbs describe a word that *implies* an action even if that word is not a standard verb in the English language, such as *New*. |
| noun | oval-def:  EntityStateStringType | 0..1 | false | The noun name of the cmdlet[[267]](#footnote-267). This noun specifies the resource[[268]](#footnote-268) that the cmdlet acts upon. |
| parameters | oval-def:  EntityStateRecordType | 0..1 | false | The parameters of the cmdlet, that is, the list of properties (name and value pairs) as input to invoke the cmdlet[[269]](#footnote-269).  Each property name must be unique. Also, parameter names SHOULD align with the MSDN documentation[[270]](#footnote-270). |
| select | oval-def:  EntityStateRecordType | 0..1 | false | A set of name and value pairs used as input to the Select-Object[[271]](#footnote-271) cmdlet in order to target output properties. Each property name MUST be unique. |
| value | oval-def:  EntityStateRecordType | 0..1 | false | The expected value represented as a set of fields (name and value pairs) that represent the data returned by executing the specified cmdlet on the system. Each field must have a unique name. |

## win-sc:cmdlet\_item

The cmdlet\_item represents a PowerShell cmdlet, the parameters supplied to it, and the value it returned[[272]](#footnote-272). Certain attributes (such as nouns, verbs, and parameter names) SHOULD align with the MSDN documentation[[273]](#footnote-273).



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| module\_name | oval-sc:EntityItemStringType | 0..1 | true | The name of the module that defines the cmdlet[[274]](#footnote-274). When set using the New-Module command in Powershell, the default name is \_\_DynamicModule\_PATHID where "PATHID" is a unique identifier that specifies the path to the dynamic module[[275]](#footnote-275).  If **xsi:nil="true"**, it implies that it does not matter which module name the command comes from. |
| module\_id | win-sc:EntityItemGUIDType | 0..1 | true | A global unique identifier (GUID) instituted so as to avoid module conflict. This is in the form A-B-C-D-E where A is an 8-digit hexadecimal number, B, C, and D are 4-digit hexadecimal numbers, and E is a 12-digit hexadecimal number[[276]](#footnote-276).  If **xsi:nil="true"**, it implies that it does not matter which module GUID the command comes from. |
| module\_version | oval-sc:EntityItemVersionType | 0..1 | true | Module version in the format of MAJOR.MINOR[[277]](#footnote-277). If **xsi:nil="true"**, it implies that it does not matter which version of the module the command refers to. |
| verb | win-sc:  EntityItemCmdletVerbType | 0..1 | false | The verb name of the cmdlet[[278]](#footnote-278). This verb specifies the action[[279]](#footnote-279) taken by the cmdlet. NOTE: In Windows Powershell, verbs describe a word that *implies* an action even if that word is not a standard verb in the English language, such as *New*. |
| noun | oval-sc:EntityItemStringType | 0..1 | false | The noun name of the cmdlet[[280]](#footnote-280). This noun specifies the resource[[281]](#footnote-281) that the cmdlet acts upon. |
| parameters | oval-sc:EntityItemRecordType | 0..1 | true | The parameters of the cmdlet, that is, the list of properties (name and value pairs) as input to invoke the cmdlet. Each property name must be unique.  If **xsi:nil="true"**, parameters are NOT provided to the cmdlet[[282]](#footnote-282). Also, parameter names SHOULD align with the MSDN documentation[[283]](#footnote-283). |
| select | oval-sc:EntityItemRecordType | 0..1 | true | A set of name and value pairs used as input to the Select-Object[[284]](#footnote-284) cmdlet in order to target output properties. Each property name MUST be unique.  If **xsi:nil="true"**, these pairs are not provided to the cmdlet. |
| value | oval-sc:EntityItemRecordType | 0..\* | false | The expected value represented as a set of fields (name and value pairs) that represent the data returned by executing the specified cmdlet on the system. . Each field must have a unique name. |

## win-def:EntityObjectGUIDType

The EntityObjectGUIDType restricts a string value to a representation of a GUID, used for module ID. The empty string is also allowed to support empty element associated with variable references. Note that when using pattern matches and variables care must be taken to ensure that the regular expression and variable values align with the specified pattern restriction.

|  |  |  |
| --- | --- | --- |
| Datatype Restriction | Additional Restrictions | Explanation |
| oval-def:EntityObjectStringType | (\{[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{12}\}){0,} | Strings with this datatype must be in the form A-B-C-D-E where A is an 8-digit hexadecimal number, B, C, and D are 4-digit hexadecimal numbers, and E is a 12-digit hexadecimal number. |
| *<empty string>* | N/A | This value indicates that no value has been specified and is permitted here to allow for an empty entity which is associated with a reference to an OVAL Variable. |

## win-def:EntityStateGUIDType

The EntityStateGUIDType restricts a string value to a representation of a GUID, used for module ID. The empty string is also allowed to support empty element associated with variable references. Note that when using pattern matches and variables care must be taken to ensure that the regular expression and variable values align with the specified pattern restriction.

|  |  |  |
| --- | --- | --- |
| Datatype Restriction | Additional Restrictions | Explanation |
| oval-def:EntityStateStringType | (\{[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{12}\}){0,} | Strings with this datatype must be in the form A-B-C-D-E where A is an 8-digit hexadecimal number, B, C, and D are 4-digit hexadecimal numbers, and E is a 12-digit hexadecimal number. |
| *<empty string>* | N/A | This value indicates that no value has been specified and is permitted here to allow for an empty entity which is associated with a reference to an OVAL Variable. |

## win-sc:EntityItemGUIDType

The EntityObjectGUIDType restricts a string value to a representation of a GUID, used for module ID. The empty string is also allowed to support empty element associated with variable references. Note that when using pattern matches and variables care must be taken to ensure that the regular expression and variable values align with the specified pattern restriction.

|  |  |  |
| --- | --- | --- |
| Datatype Restriction | Additional Restrictions | Explanation |
| oval-sc:EntityItemStringType | (\{[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{12}\}){0,} | Strings with this datatype must be in the form A-B-C-D-E where A is an 8-digit hexadecimal number, B, C, and D are 4-digit hexadecimal numbers, and E is a 12-digit hexadecimal number. |
| *<empty string>* | N/A | This value indicates that no value has been specified and is permitted here to allow for an empty entity which is associated with a reference to an OVAL Variable. |

## win-def:EntityObjectCmdletVerbType

The EntityObjectCmdletVerbType restricts a string value to a set of allow cmdlet verbs. The empty string is also allowed to support empty element associated with variable references. Note that when using pattern matches and variables care must be taken to ensure that the regular expression and variable values align with the specified pattern restriction.

|  |  |
| --- | --- |
| Enumeration Value | Description |
| Approve | The Approve verb confirms or agrees to the status of a resource or process. |
| Assert | The Assert verb affirms the state of a resource. |
| Compare | The Compare verb evaluates the data from one resource against the data from another resource. |
| Confirm | The Confirm verb acknowledges, verifies, or validates, the state of a resource or process. |
| Find | The Find verb looks for an object in a container that is unknown, implied, optional, or specified. |
| Get | The Get verb specifies an action that retrieves a resource. |
| Import | The Import verb creates a resource from data that is stored in a persistent data store (such as a file) or in an interchange format. |
| Measure | The Measure verb identifies resources that are consumed by a specified operation, or retrieves statistics about a resource. |
| Read | The Read verb acquires information from a source. |
| Request | The Request verb asks for a resource or asks for permissions. |
| Resolve | The Resolve verb maps a shorthand representation of a resource to a more complete representation. |
| Search | The Search verb creates a reference to a resource in a container. |
| Select | The Select verb locates a resource in a container. |
| Show | The Show verb makes a resource visible to the user. |
| Test | The Test verb verifies the operation or consistency of a resource. |
| Trace | The Trace verb tracks the activities of a resource. |
| Watch | The Watch verb continually inspects or monitors a resource for changes. |
| *<empty string>* | This value indicates that no value has been specified and is permitted here to allow for an empty entity which is associated with a reference to an OVAL Variable. |

## win-def:EntityStateCmdletVerbType

The EntityStateCmdletVerbType restricts a string value to a set of allow cmdlet verbs. The empty string is also allowed to support empty element associated with variable references. Note that when using pattern matches and variables care must be taken to ensure that the regular expression and variable values align with the specified pattern restriction.

|  |  |
| --- | --- |
| Enumeration Value | Description |
| Approve | The Approve verb confirms or agrees to the status of a resource or process. |
| Assert | The Assert verb affirms the state of a resource. |
| Compare | The Compare verb evaluates the data from one resource against the data from another resource. |
| Confirm | The Confirm verb acknowledges, verifies, or validates, the state of a resource or process. |
| Find | The Find verb looks for an object in a container that is unknown, implied, optional, or specified. |
| Get | The Get verb specifies an action that retrieves a resource. |
| Import | The Import verb creates a resource from data that is stored in a persistent data store (such as a file) or in an interchange format. |
| Measure | The Measure verb identifies resources that are consumed by a specified operation, or retrieves statistics about a resource. |
| Read | The Read verb acquires information from a source. |
| Request | The Request verb asks for a resource or asks for permissions. |
| Resolve | The Resolve verb maps a shorthand representation of a resource to a more complete representation. |
| Search | The Search verb creates a reference to a resource in a container. |
| Select | The Select verb locates a resource in a container. |
| Show | The Show verb makes a resource visible to the user. |
| Test | The Test verb verifies the operation or consistency of a resource. |
| Trace | The Trace verb tracks the activities of a resource. |
| Watch | The Watch verb continually inspects or monitors a resource for changes. |
| *<empty string>* | This value indicates that no value has been specified and is permitted here to allow for an empty entity which is associated with a reference to an OVAL Variable. |

## win-sc:EntityItemCmdletVerbType

The EntityItemCmdletVerbType restricts a string value to a set of allow cmdlet verbs. The empty string is also allowed to support empty element associated with variable references. Note that when using pattern matches and variables care must be taken to ensure that the regular expression and variable values align with the specified pattern restriction.

|  |  |
| --- | --- |
| Enumeration Value | Description |
| Approve | The Approve verb confirms or agrees to the status of a resource or process. |
| Assert | The Assert verb affirms the state of a resource. |
| Compare | The Compare verb evaluates the data from one resource against the data from another resource. |
| Confirm | The Confirm verb acknowledges, verifies, or validates, the state of a resource or process. |
| Find | The Find verb looks for an object in a container that is unknown, implied, optional, or specified. |
| Get | The Get verb specifies an action that retrieves a resource. |
| Import | The Import verb creates a resource from data that is stored in a persistent data store (such as a file) or in an interchange format. |
| Measure | The Measure verb identifies resources that are consumed by a specified operation, or retrieves statistics about a resource. |
| Read | The Read verb acquires information from a source. |
| Request | The Request verb asks for a resource or asks for permissions. |
| Resolve | The Resolve verb maps a shorthand representation of a resource to a more complete representation. |
| Search | The Search verb creates a reference to a resource in a container. |
| Select | The Select verb locates a resource in a container. |
| Show | The Show verb makes a resource visible to the user. |
| Test | The Test verb verifies the operation or consistency of a resource. |
| Trace | The Trace verb tracks the activities of a resource. |
| Watch | The Watch verb continually inspects or monitors a resource for changes. |
| *<empty string>* | This value indicates that no value has been specified and is permitted here to allow for an empty entity which is associated with a reference to an OVAL Variable. |

## win-def:user\_test

The user\_test is used to retrieve information about Windows users and which security groups they belong to. When the user\_test collects data on the users of the system, it typically includes the local and built-in user accounts and not domain user accounts. However, it is important to note that domain user accounts can still be accessed. The user\_test MUST reference one user\_object and zero or more user\_states[[285]](#footnote-285).



### Known Supported Platforms

* Windows XP
* Windows Vista
* Windows 7

## win-def:user\_object

The user\_object construct defines the set of users whose information should be collected and represented as user\_items.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| set | oval-def:set | 0..1 | false | Enables the expression of complex user\_objects that are the result of logically combining and filtering the user\_items that are identified by one or more user\_objects. Please see the OVAL Language Specification for additional information. |
| user | oval-def:  EntityObjectStringType | 1..1 | false | The user property holds a case-insensitive string that represents the name of a particular user.  In a domain environment, users SHOULD be identified in the form: "domain\user name". For local users use: "computer name\user name". For built-in accounts on the system, use the user name without a domain. User account names SHOULD align with the MSDN documentation[[286]](#footnote-286).  In particular, user account names in Windows are limited to 20 characters and SHOULD NOT contain the following illegal characters in the set {", /, \, [, ], :, |, <, >, +, =, ;, ?, \*}, any commas, or non-printable ASCII characters in the range 1-31. |
| filter | oval-def:filter | 0..\* | false | Allows for the explicit inclusion or exclusion of user\_items from the set of user\_items collected by a user\_object. Please see the OVAL Language Specification for additional information. |

## win-def:user\_state

The user\_state construct is used by a user\_test to specify user\_item attribute criteria to check on Microsoft Windows platforms.



|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Property | Type | | Multiplicity | | Nillable | | Description |
| user | oval-def:  EntityStateStringType | 0..1 | | false | | The user property holds a case-insensitive string that represents the name of a particular user.  In a domain environment, users SHOULD be identified in the form: "domain\user name". For local users use: "computer name\user name".  For built-in accounts on the system, use the user name without a domain. User account names SHOULD align with the MSDN documentation[[287]](#footnote-287).  In particular, user account names in Windows are limited to 20 characters and SHOULD NOT contain the following illegal characters in the set {", /, \, [, ], :, |, <, >, +, =, ;, ?, \*}, any commas, or non-printable ASCII characters in the range 1-31. | |
| enabled | oval-def:EntityStateBoolType | 0..1 | | false | | This property holds a boolean value that is *true* if the particular user account is enabled or *false* if it is not enabled. | |
| group | oval-def:  EntityStateStringType | 0..1 | | false | | A case insensitive string that represents the name of a particular group.  In a domain environment, groups should be identified in the form: "domain\group name". For local groups use: "computer name\group name". For built-in accounts on the system, use the group name without a domain.  Group names SHOULD align with the MSDN documentation[[288]](#footnote-288).  In particular, group names in Windows are limited to 256 characters and SHOULD NOT contain the following illegal characters in the set {", /, \, [, ], :, |, <, >, +, =, ;, ?, \*}, any commas, or non-printable ASCII characters in the range 1-31. | |
| last\_login | oval-def:EntityStateIntType | 0..1 | | true | | The date and time when the last logon occurred. This value is stored as the number of seconds that have elapsed since 00:00:00, January 1, 1970, GMT. | |

## win-sc:user\_item

The Windows user\_item allows for the collection of the different groups (identified by name) a user belongs to.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| user | oval-sc:  EntityItemStringType | 0..1 | false | The user property holds a case-insensitive string that represents the name of a particular user.  In a domain environment, users will be identified in the form: "domain\user name". For local users: "computer name\user name" is used. For built-in accounts on the system, the user name is used without a domain.  User account names SHOULD align with the MSDN documentation[[289]](#footnote-289). In particular, user account names in Windows are limited to 20 characters and SHOULD NOT contain the following illegal characters in the set {", /, \, [, ], :, |, <, >, +, =, ;, ?, \*}, any commas, or non-printable ASCII characters in the range 1-31. |
| enabled | oval-sc:  EntityItemBoolType | 0..1 | false | This element holds a boolean value that is *true* if the particular user account is enabled or *false* if it is not enabled. |
| group | oval-sc:  EntityItemStringType | 0..\* | false | A string that represents the name of a particular group.  The group element can be included multiple times in a system characteristic item in order to record that a user can be a member of a number of different groups.  Group names SHOULD align with the MSDN documentation[[290]](#footnote-290). In particular, group names in Windows are limited to 256 characters and SHOULD NOT contain the following illegal characters in the set {", /, \, [, ], :, |, <, >, +, =, ;, ?, \*}, any commas, or non-printable ASCII characters in the range 1-31. |
| last\_login | oval-sc:  EntityItemIntType | 0..1 | false | The date and time when the last logon occurred. This value is stored as the number of seconds that have elapsed since 00:00:00, January 1, 1970, GMT. |

## win-def:user\_sid55\_test

The user\_sid55\_test is used to retrieve information about Windows users, identified by their SID, and which security groups they belong to. Use the user\_test instead to retrieve information on users using their name. When the user\_sid55\_test collects data on the users of the system, it typically includes the local and built-in user accounts and not domain user accounts. However, it is important to note that domain user accounts can still be accessed. The user\_sid55\_test MUST reference one user\_sid55\_object and zero or more user\_sid55\_states[[291]](#footnote-291).



### Known Supported Platforms

* Windows XP
* Windows Vista
* Windows 7

## win-def:user\_sid55\_object

The user\_sid55\_object construct defines the set of users whose information should be collected and represented as user\_sid\_items.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| set | oval-def:set | 0..1 | false | Enables the expression of complex user\_sid55\_objects that are the result of logically combining and filtering the user\_sid\_items that are identified by one or more user\_sid55\_objects. Please see the OVAL Language Specification for additional information. |
| user\_sid | oval-def:EntityObjectStringType | 1..1 | false | The user attribute holds a string that represents the SID of a particular user. |
| filter | oval-def:filter | 0..\* | false | Allows for the explicit inclusion or exclusion of user\_items from the set of user\_items collected by a user\_object. Please see the OVAL Language Specification for additional information. |

## win-def:user\_sid55\_state

The user\_sid55\_state construct is used by a user\_sid55\_test to specify user\_sid\_item attribute criteria to check on Microsoft Windows platforms.



|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Property | Type | | Multiplicity | | Nillable | | Description |
| user\_sid | oval-def:EntityStateStringType | 0..1 | | false | | The user property holds a string that represents the SID of a particular user. | |
| enabled | oval-def:EntityStateBoolType | 0..1 | | false | | This element holds a boolean value that is *true* if the particular user account is enabled or *false* if it is not enabled. | |
| group\_sid | oval-def:EntityStateStringType | 0..1 | | false | | A string that represents the SID of a particular group. | |

## win-sc:user\_sid\_item

The windows user\_sid\_item allows the different groups (identified by SID) that a user belongs to, to be collected.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| user\_sid | oval-sc:  EntityItemStringType | 0..1 | false | The user property holds a string that represents the SID of a particular user. |
| enabled | oval-sc:  EntityItemBoolType | 0..1 | false | This element holds a boolean value that is *true* if the particular user account is enabled or *false* if it is not enabled. |
| group\_sid | oval-sc:  EntityItemStringType | 0..\* | false | A string that represents the SID of a group to which the user belongs. |

## win-def:wmi\_test

The wmi\_test is used to make assertions about information accessed by WMI[[292]](#footnote-292). The wmi\_test MUST reference one wmi\_object and zero or more wmi\_states.  


### Known Supported Platforms

* Windows XP
* Windows Vista
* Windows 7

## win-def:wmi\_object

The wmi\_object construct defines the applicable WMI information that should be collected and represented as wmi57\_items[[293]](#footnote-293). It allows for single fields to be selected from WMI.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| set | oval-def:set | 0..1 | false | Enables the expression of complex wmi57\_objects that are the result of logically combining and filtering the wmi57\_items that are identified by one or more wmi57\_objects. |
| namespace | oval-def:EntityObjectStringType | 0..1 | false | Specifies which WMI namespace to look under. Each WMI provider normally registers its own WMI namespace and then all its classes within that namespace[[294]](#footnote-294). |
| wql | oval-def:EntityObjectStringType | 0..1 | false | A WQL query used to identify the wmi\_objects to represent as wmi\_items. Any valid WQL query is usable with one exception, at most one field is allowed in the SELECT portion of the query[[295]](#footnote-295). |
| filter | oval-def:filter [2] | 0..\* | false | Allows for the explicit inclusion or exclusion of wmi\_items from the set of wmi\_items collected by a wmi\_object. Please see the OVAL Language Specification [2] for additional information. |

## win-def:wmi\_state

The wmi\_state construct is used by a wmi\_test to outline information to be checked through Microsoft's WMI interface. It specifies the applicable WMI information that can be associated with a given wmi57\_object under Microsoft Windows platforms[[296]](#footnote-296).



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| namespace | oval-def:  EntityStateStringType | 0..1 | false | Specifies which WMI namespace to look under. Each WMI provider normally registers its own WMI namespace and then all its classes within that namespace[[297]](#footnote-297). |
| wql | oval-def:  EntityStateStringType | 0..1 | false | A WQL query used to identify the wmi\_objects to represent as wmi\_items. Any valid WQL query is usable with one exception, at most one field is allowed in the SELECT portion of the query[[298]](#footnote-298). |
| result | oval-def:  EntityStateRecordType | 0..1 | false | The result attribute specifies how to test items in the result set of the specified WQL statement under the WQL property. |

## win-sc:wmi\_item

The wmi\_item outlines information to be checked through Microsoft's WMI interface.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| namespace | oval-sc:  EntityItemStringType | 0..1 | false | Specifies which WMI namespace to look under. Each WMI provider normally registers its own WMI namespace and then all its classes within that namespace[[299]](#footnote-299). |
| wql | oval-sc:  EntityItemStringType | 0..1 | false | A WQL query used to identify the wmi\_objects to represent as wmi\_items. Any valid WQL query is usable with one exception, at most one field is allowed in the SELECT portion of the query[[300]](#footnote-300). |
| result | oval-sc:  EntityItemRecordType | 0..\* | false | The result attribute specifies how to test items in the result set of the specified WQL statement under the WQL property. |

## win-def:group\_test

The group\_test allows for the testing of different users and subgroups that directly belong to specific groups[[301]](#footnote-301). A subgroup is an account identified by SID (not by name) that is of group type, which can be seen when the SID\_NAME\_TYPE enumeration value of SidTypeGroup, or 2, is obtained when inputting a SID into the LookupAccountSid function[[302]](#footnote-302).

When the group\_test collects the groups on the system, it should only include the local and built-in group accounts and not domain group accounts. However, it is important to note that domain group accounts can still be looked up. Also, note that the subgroups of the group will not be resolved to find indirect user and group members. If the subgroups need to be resolved, it should be done using the sid\_object. The group\_test MUST reference one group\_object and zero or more group\_states.



### Known Supported Platforms

* Windows XP
* Windows Vista
* Windows 7

## win-def:group\_object

The group\_object is used by a group\_test to define the specific group(s) (identified by name) to be evaluated and represented as group\_items.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| set | oval-def:set | 0..1 | false | Enables the expression of complex group\_objects that are the result of logically combining and filtering the group\_items that are identified by one or more group\_objects. Please see the OVAL Language Specification for additional information. |
| group | oval-def:  EntityObjectStringType | 1..1 | false | A case insensitive string that represents the name of a particular group.  In a domain environment, groups should be identified in the form: "domain\group name". For local groups use: "computer name\group name". For built-in accounts on the system, use the group name without a domain.  Group names SHOULD align with the MSDN documentation[[303]](#footnote-303). In particular, group names in Windows are limited to 256 characters and SHOULD NOT contain the following illegal characters in the set {", /, \, [, ], :, |, <, >, +, =, ;, ?, \*}, any commas, or non-printable ASCII characters in the range 1-31. |
| filter | oval-def:filter | 0..\* | false | Allows for the explicit inclusion or exclusion of group\_items from the set of group\_items collected by a group\_object. Please see the OVAL Language Specification for additional information. |

## win-def:group\_state

The group\_state construct is used by a group\_test to specify group\_item attribute criteria to check on Microsoft Windows platforms.



|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Property | Type | | Multiplicity | | Nillable | | Description |
| group | oval-def:  EntityStateStringType | 0..1 | | false | | A case insensitive string that represents the name of a particular group.  In a domain environment, groups should be identified in the form: "domain\group name". For local groups use: "computer name\group name". For built-in accounts on the system, use the group name without a domain.  Group names SHOULD align with the MSDN documentation[[304]](#footnote-304). In particular, group names in Windows are limited to 256 characters and SHOULD NOT contain the following illegal characters in the set {", /, \, [, ], :, |, <, >, +, =, ;, ?, \*}, any commas, or non-printable ASCII characters in the range 1-31. | |
| user | oval-def:  EntityStateStringType | 0..1 | | false | | A case-insensitive string that represents the name of a particular user.  In a domain environment, users will be identified in the form: "domain\user name". For local users: "computer name\user name" is used. For built-in accounts on the system, the user name is used without a domain.  User account names SHOULD align with the MSDN documentation[[305]](#footnote-305). In particular, user account names in Windows are limited to 20 characters and SHOULD NOT contain the following illegal characters in the set {", /, \, [, ], :, |, <, >, +, =, ;, ?, \*}, any commas, or non-printable ASCII characters in the range 1-31. | |
| subgroup | oval-def:  EntityStateStringType | 0..1 | | false | | A case-insensitive string that represents the name of a particular subgroup in the context of the specified group.  In a domain environment, subgroups should be identified in the form: "domain\subgroup name". For local groups use: "computer name\subgroup name". If the subgroups are built-in groups, use the subgroup name without a domain component.  Because a subgroup in Windows is still considered a group, subgroup names SHOULD align with the MSDN documentation[[306]](#footnote-306).  Thus, subgroup names are limited to 256 characters and SHOULD NOT contain the following illegal characters in the set {", /, \, [, ], :, |, <, >, +, =, ;, ?, \*}, any commas, or non-printable ASCII characters in the range 1-31. | |

## win-sc:group\_item

The Windows group\_item allows for the collection of the different groups (identified by name) that a user belongs to. The Windows group\_item allows the different users and subgroups, that directly belong to specific groups (identified by name), to be collected. The collected subgroups will not be resolved to find indirect user or subgroup members. If the subgroups need to be resolved, it should be done using the sid\_object.

Note that the user and subgroup elements can appear an unlimited number of times. If a user is not found in the specified group, a single user element should exist with a status of 'does not exist'. If there is an error determining the users of a group, a single user element should exist with a status of 'error'. If a subgroup is not found in the specified group, a single subgroup element should exist with a status of 'does not exist'. If there is an error determining the subgroups of a group, a single subgroup element should exist with a status of 'error'.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| group | oval-sc:  EntityItemStringType | 0..1 | false | A case insensitive string that represents the name of a particular group.  In a domain environment, groups should be identified in the form: "domain\group name". For local groups use: "computer name\group name". For built-in accounts on the system, use the group name without a domain.  Group names SHOULD align with the MSDN documentation[[307]](#footnote-307). In particular, group names in Windows are limited to 256 characters and SHOULD NOT contain the following illegal characters in the set {", /, \, [, ], :, |, <, >, +, =, ;, ?, \*}, any commas, or non-printable ASCII characters in the range 1-31. |
| user | oval-sc:  EntityItemStringType | 0..\* | false | A case-insensitive string that represents the name of a particular user.  In a domain environment, users will be identified in the form: "domain\user name". For local users: "computer name\user name" is used. For built-in accounts on the system, the user name is used without a domain.  User account names SHOULD align with the MSDN documentation[[308]](#footnote-308). In particular, user account names in Windows are limited to 20 characters and SHOULD NOT contain the following illegal characters in the set {", /, \, [, ], :, |, <, >, +, =, ;, ?, \*}, any commas, or non-printable ASCII characters in the range 1-31. |
| subgroup | oval-sc:  EntityItemStringType | 0..\* | false | A case-insensitive string that represents the name of a particular subgroup in the context of the specified group.  In a domain environment, subgroups should be identified in the form: "domain\subgroup name". For local groups use: "computer name\subgroup name". If the subgroups are built-in groups, use the subgroup name without a domain component.  Because a subgroup in Windows is still considered a group, subgroup names SHOULD align with the MSDN documentation[[309]](#footnote-309).  Thus, subgroup names are limited to 256 characters and SHOULD NOT contain the following illegal characters in the set {", /, \, [, ], :, |, <, >, +, =, ;, ?, \*}, any commas, or non-printable ASCII characters in the range 1-31. |

## win-def:group\_sid\_test

The group\_sid\_test allows the different users and subgroups, that directly belong to specific groups (identified by SID), to be tested. A subgroup is an account identified by SID (not by name) that is of group type, which can be seen when the SID\_NAME\_TYPE enumeration value of SidTypeGroup, or 2, is obtained when inputting a SID into the LookupAccountSid function[[310]](#footnote-310).

When the group\_sid\_test collects the groups on the system, it should only include the local and built-in group SIDs and not domain group SIDs. However, it is important to note that domain group accounts can still be looked up. Also, note that the subgroups of the group will not be resolved to find indirect user and group members. If the subgroups need to be resolved, it should be done using the sid\_sid\_object. The group\_sid\_test MUST reference one group\_sid\_object and zero or more group\_sid\_states.



### Known Supported Platforms

* Windows XP
* Windows Vista
* Windows 7

## win-def:group\_sid\_object

The group\_sid\_object is used by a group\_sid\_test to define the specific group(s) (identified by SID) to be evaluated and represented as group\_sid\_items.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| set | oval-def:set | 0..1 | false | Enables the expression of complex group\_sid\_objects that are the result of logically combining and filtering the group\_sid\_items that are identified by one or more group\_sid\_objects. Please see the OVAL Language Specification for additional information. |
| group\_sid | oval-def:  EntityObjectStringType | 1..1 | false | The group\_sid attribute holds a string that represents the SID of a particular group. |
| filter | oval-def:filter | 0..\* | false | Allows for the explicit inclusion or exclusion of group\_sid\_items from the set of group\_sid\_items collected by a group\_sid\_object. Please see the OVAL Language Specification for additional information. |

## win-def:group\_sid\_state

The group\_sid\_state construct is used by a group\_sid\_test to specify group\_sid\_item attribute criteria to check on Microsoft Windows platforms. This test enumerates the different users and subgroups directly associated with a Windows group.



|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Property | Type | | Multiplicity | | Nillable | | Description |
| group\_sid | oval-def:  EntityStateStringType | 0..1 | | false | | The group\_sid property holds a string attribute that represents the SID of a particular group. | |
| user\_sid | oval-def:  EntityStateStringType | 0..1 | | false | | The user property represents the SID of a particular user. | |
| subgroup\_sid | oval-def:  EntityStateStringType | 0..1 | | false | | The subgroup\_sid property holds a string that represents the SID of particular subgroup in the specified group. | |

## win-sc:group\_sid\_item

The Windows group\_sid\_item allows the different users and subgroups, that directly belong to specific groups (identified by SID), to be collected. The collected subgroups will not be resolved to find indirect user or subgroup members. If the subgroups need to be resolved, it should be done using the sid\_object. Note that the user and subgroup elements can appear an unlimited number of times. If a user is not found in the specified group, a single user element should exist with a status of 'does not exist'. If there is an error determining the users of a group, a single user element should exist with a status of 'error'. If a subgroup is not found in the specified group, a single subgroup element should exist with a status of 'does not exist'. If there is an error determining the subgroups of a group, a single subgroup element should exist with a status of 'error'.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| group\_sid | oval-sc:  EntityItemStringType | 0..1 | false | The group\_sid construct holds string that represents the SID of a particular group. |
| user\_sid | oval-sc:  EntityItemStringType | 0..\* | false | The user construct represents the SID of a particular user. |
| subgroup\_sid | oval-sc:  EntityItemStringType | 0..\* | false | The subgroup\_sid entity holds a string that represents the SID of particular subgroup in the specified group. |

## win-def:metabase\_test

The metabase\_test is used to make assertions about information[[311]](#footnote-311) found in the Windows metabase[[312]](#footnote-312). The metabase\_test MUST reference one metabase\_object and zero or more metabase\_states.  


### Known Supported Platforms

* Windows XP
* Windows Vista
* Windows 7

## win-def:metabase\_object

The metabase\_object construct defines the applicable metabase information that should be collected and represented as metabase\_items[[313]](#footnote-313).



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| set | oval-def:set | 0..1 | false | Enables the expression of complex metabase\_objects that are the result of logically combining and filtering the metabase\_items that are identified by one or more metabase\_objects. |
| key | oval-def:EntityObjectStringType | 0..1 | false | This attribute specifies a metabase key[[314]](#footnote-314). |
| id | oval-def:EntityObjectIntType | 0..1 | true | This attribute specifies a particular object under the metabase key [[315]](#footnote-315). If **xsi:nil=true**, then the object being specified is the higher level key. In this case, the id element SHOULD NOT be collected or used in analysis. |
| filter | oval-def:filter [2] | 0..\* | false | Allows for the explicit inclusion or exclusion of metabase\_items from the set of metabase\_items collected by a metabase \_object. Please see the OVAL Language Specification [2] for additional information. |

## win-def:metabase\_state

The metabase\_state construct is used by a metabase\_test to outline information to be checked through Microsoft's WMI interface. It specifies the applicable WMI information that can be associated with a given metabase\_object under Microsoft Windows platforms. Some metabase properties can be found via the METADATA\_RECORD[[316]](#footnote-316). The alternate names refer to the variables used in the METADATA\_RECORD[[317]](#footnote-317) structure corresponding to specific properties used here.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| key | oval-def:  EntityStateStringType | 0..1 | false | This attribute specifies a metabase key[[318]](#footnote-318). |
| id | oval-def:  EntityStateIntType | 0..1 | false | This attribute specifies a particular object under the metabase key [[319]](#footnote-319). |
| name | oval-def:  EntityStateStringType | 0..1 | false | This attribute describes the name of the specified metabase object. |
| user\_type | oval-def:  EntityStateStringType | 0..1 | false | Alternate name: dwMDUserType. This attribute is an integer value that specifies the user type of the data[[320]](#footnote-320). |
| data\_type | oval-def:  EntityStateStringType | 0..1 | false | Alternate name: dwMDDataType. The data\_type element identifies the type of data in the metabase entry[[321]](#footnote-321). |
| data | oval-def:  EntityStateAnySimpleType | 0..1 | false | Alternate name: The actual data of the named item under the specified metabase key[[322]](#footnote-322). This includes property attributes, usertype, datatype number of data entries, and others that can be obtained via the GetAllData method[[323]](#footnote-323) . |

## win-sc:metabase\_item

The metabase\_item gathers information from the specified metabase keys[[324]](#footnote-324).



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| key | oval-sc:  EntityItemStringType | 0..1 | false | This attribute specifies a metabase key[[325]](#footnote-325). |
| id | oval-sc:EntityItemIntType | 0..1 | true | This attribute specifies a particular object under the metabase key [[326]](#footnote-326). |
| name | oval-sc:  EntityItemStringType | 0..1 | false | This attribute describes the name of the specified metabase object. |
| user\_type | oval-sc:  EntityItemStringType | 0..1 | false | Alternate name: dwMDUserType. This attribute is an integer value that specifies the user type of the data[[327]](#footnote-327). |
| data\_type | oval-sc:  EntityItemStringType | 0..1 | false | Alternate name: dwMDDataType. The data\_type element identifies the type of data in the metabase entry[[328]](#footnote-328). |
| data | oval-sc:  EntityItemAnySimpleType | 0..\* | false | Alternate name: The actual data of the named item under the specified metabase key[[329]](#footnote-329). This includes property attributes, usertype, datatype number of data entries, and others that can be obtained via the GetAllData method[[330]](#footnote-330) . |

## win-def:process\_test

The process\_test is used to make assertions about information found in Windows processes[[331]](#footnote-331). The process\_test MUST reference one process\_object and zero or more process\_states.   


### Known Supported Platforms

* Windows XP
* Windows Vista
* Windows 7

## win-def:process\_object

The process\_object construct defines the applicable process information that should be collected and represented as process\_items.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| set | oval-def:set | 0..1 | false | Enables the expression of complex process\_objects that are the result of logically combining and filtering the process\_items that are identified by one or more process\_objects. |
| command\_line | oval-def:  EntityObjectStringType | 0..1 | false | The string used to start the process[[332]](#footnote-332).  This includes any parameters that are part of the command line. |
| filter | oval-def:filter [2] | 0..\* | false | Allows for the explicit inclusion or exclusion of process\_items from the set of process\_items collected by a process \_object. Please see the OVAL Language Specification [2] for additional information. |

## win-def:process\_state

The process\_state construct is used by a process\_test to outline information about Windows processes[[333]](#footnote-333). By hitting CTRL-ALT-DELETE and clicking "Start Task Manager," a system administrator can view the contents of the properties specified here. If they are not shown, go to View->Select Columns… and select the fields corresponding to the "alternate names" mentioned here.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| command\_line | oval-def:  EntityStateStringType | 0..1 | false | Alternate name: Command Line. The string used to start the process[[334]](#footnote-334). This includes any parameters that are part of the command line. |
| pid | oval-def:EntityStateIntType | 0..1 | false | Alternate name: PID. The ID given to the process that is created for a specific command line. |
| ppid | oval-def:EntityStateIntType | 0..1 | false | The ID given to the parent of the process that is created for the specified command line. |
| priority | oval-def:  EntityStateStringType | 0..1 | false | Alternate name: Base Priority. The base priority of the process. |
| image\_path | oval-def:  EntityStateStringType | 0..1 | false | Alternate name: Image Name. The name of the executable file in question. If it is 32-bit, the "Image Name" does not contain the "\* 32" part of the name. |
| current\_dir | oval-def:  EntityStateStringType | 0..1 | false | Alternate name: Image Path Name, but without the file part. The current path to the executable, NOT including the exectable name itself.  In other words, if y.exe was found in path x:\, then image\_path would return y.exe and current\_dir would return x:\. Image Path Name returns x:\y.exe in Task Manager. |

## win-sc:process\_item

The process\_item gathers information from the specified Windows processes[[335]](#footnote-335). By hitting CTRL-ALT-DELETE and clicking "Start Task Manager," a system administrator can view the contents of most of the properties specified here (not including command line). If they are not shown, go to View->Select Columns… and select the fields corresponding to the "alternate names" mentioned here.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Property | Type | Multiplicity | Nillable | Description |
| command\_line | oval-sc:  EntityItemStringType | 0..1 | false | Alternate name: Command Line. The string used to start the process[[336]](#footnote-336). This includes any parameters that are part of the command line. |
| pid | oval-sc:EntityItemIntType | 0..1 | false | Alternate name: PID. The ID given to the process that is created for a specific command line. |
| ppid | oval-sc:EntityItemIntType | 0..1 | false | The ID given to the parent of the process that is created for the specified command line. |
| priority | oval-sc:  EntityItemStringType | 0..1 | false | Alternate name: Base Priority. The base priority of the process. |
| image\_path | oval-sc:  EntityItemStringType | 0..1 | false | Alternate name: Image Name. The name of the executable file in question. If it is 32-bit, the "Image Name" does not contain the "\* 32" part of the name. |
| current\_dir | oval-sc:  EntityItemStringType | 0..1 | false | Alternate name: Image Path Name, but without the file part. The current path to the executable, NOT including the exectable name itself.  In other words, if y.exe was found in path x:\, then image\_path would return y.exe and current\_dir would return x:\. Image Path Name returns x:\y.exe in Task Manager. |

# Appendix A – Normative References

[1] RFC 2119 – Key words for use in RFCs to Indicate Requirement Levels

<http://www.ietf.org/rfc/rfc2119.txt>

[2] The OVAL Language Specification

<http://oval.mitre.org/language/version5.10#specification>

# Appendix B - Change Log

**Version 5.11 Revision 1 – February 20, 2013**

* Added documentation clarifying that the last\_write\_time entity in the win-def:registry\_test only represents the last time a key or any of its values were modified. This addresses <https://github.com/OVALProject/Language/issues/15>.
* Updated version and date information for 5.11 Draft 1.

**Version 5.10 Revision 1 – January 19, 2012**

* Published initial revision of the version 5.10.1 Windows extension specification.

# Appendix C - Terms and Acronyms

1. For more information see <https://oval.mitre.org/about/termsofuse.html> [↑](#footnote-ref-1)
2. For more information see <https://oval.mitre.org/> [↑](#footnote-ref-2)
3. For more information see <http://en.wikipedia.org/wiki/Namespace_(computer_science)> [↑](#footnote-ref-3)
4. For more information see <http://msdn.microsoft.com/en-us/library/aa364407(v=VS.85).aspx> [↑](#footnote-ref-4)
5. For more information see <http://msdn.microsoft.com/en-us/library/aa365247.aspx> [↑](#footnote-ref-5)
6. For more information see <http://msdn.microsoft.com/en-us/library/aa365247.aspx> [↑](#footnote-ref-6)
7. For more information see <http://msdn.microsoft.com/en-us/library/aa365247.aspx> [↑](#footnote-ref-7)
8. For more information see <http://msdn.microsoft.com/en-us/library/aa384187(v=vs.85).aspx> [↑](#footnote-ref-8)
9. For more information see <http://msdn.microsoft.com/en-us/library/aa365247.aspx> [↑](#footnote-ref-9)
10. For more information see <http://msdn.microsoft.com/en-us/library/aa365247.aspx> [↑](#footnote-ref-10)
11. For more information see <http://msdn.microsoft.com/en-us/library/aa365247.aspx> [↑](#footnote-ref-11)
12. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa446654(v=vs.85).aspx>

    [↑](#footnote-ref-12)
13. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379166(v=vs.85).aspx> [↑](#footnote-ref-13)
14. For more information see <http://msdn.microsoft.com/en-us/library/14h5k7ff(v=vs.71).aspx> [↑](#footnote-ref-14)
15. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa364957(v=VS.85).aspx> [↑](#footnote-ref-15)
16. For more information see <http://msdn.microsoft.com/en-us/library/ms724284(VS.85).aspx> [↑](#footnote-ref-16)
17. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms724320(v=vs.85).aspx> [↑](#footnote-ref-17)
18. For more information see <http://msdn.microsoft.com/en-us/library/ms724284(VS.85).aspx> [↑](#footnote-ref-18)
19. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms724320(v=vs.85).aspx> [↑](#footnote-ref-19)
20. For more information see <http://msdn.microsoft.com/en-us/library/ms724284(VS.85).aspx> [↑](#footnote-ref-20)
21. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms724320(v=vs.85).aspx> [↑](#footnote-ref-21)
22. For more information see <http://msdn.microsoft.com/en-us/library/ms680355(VS.85).aspx> [↑](#footnote-ref-22)
23. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464(v=vs.85).aspx> [↑](#footnote-ref-23)
24. For more information see <http://msdn.microsoft.com/en-us/library/system.diagnostics.fileversioninfo.aspx> [↑](#footnote-ref-24)
25. For more information see <http://msdn.microsoft.com/en-us/library/aa364960(VS.85).aspx> [↑](#footnote-ref-25)
26. For more information see <http://msdn.microsoft.com/en-us/library/aa364946(VS.85).aspx> [↑](#footnote-ref-26)
27. For more information see <http://support.microsoft.com/kb/824994> [↑](#footnote-ref-27)
28. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464(v=vs.85).aspx> [↑](#footnote-ref-28)
29. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464(v=vs.85).aspx> [↑](#footnote-ref-29)
30. For more information see <http://msdn.microsoft.com/en-us/library/system.diagnostics.fileversioninfo.aspx> [↑](#footnote-ref-30)
31. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464(v=vs.85).aspx> [↑](#footnote-ref-31)
32. For more information see <http://msdn.microsoft.com/en-us/library/system.diagnostics.fileversioninfo.aspx> [↑](#footnote-ref-32)
33. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464(v=vs.85).aspx> [↑](#footnote-ref-33)
34. For more information see <http://msdn.microsoft.com/en-us/library/system.diagnostics.fileversioninfo.aspx> [↑](#footnote-ref-34)
35. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464(v=vs.85).aspx> [↑](#footnote-ref-35)
36. For more information see <http://msdn.microsoft.com/en-us/library/system.diagnostics.fileversioninfo.aspx> [↑](#footnote-ref-36)
37. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464(v=vs.85).aspx> [↑](#footnote-ref-37)
38. For more information see <http://msdn.microsoft.com/en-us/library/system.diagnostics.fileversioninfo.aspx> [↑](#footnote-ref-38)
39. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464(v=vs.85).aspx> [↑](#footnote-ref-39)
40. For more information see <http://msdn.microsoft.com/en-us/library/system.diagnostics.fileversioninfo.aspx> [↑](#footnote-ref-40)
41. For more information see <http://msdn.microsoft.com/en-us/library/aa384187(v=vs.85).aspx> [↑](#footnote-ref-41)
42. For more information see <http://msdn.microsoft.com/en-us/library/aa365247.aspx> [↑](#footnote-ref-42)
43. For more information see <http://msdn.microsoft.com/en-us/library/aa365247.aspx> [↑](#footnote-ref-43)
44. For more information see <http://msdn.microsoft.com/en-us/library/aa365247.aspx> [↑](#footnote-ref-44)
45. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa446654(v=vs.85).aspx> [↑](#footnote-ref-45)
46. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379166(v=vs.85).aspx> [↑](#footnote-ref-46)
47. For more information see <http://msdn.microsoft.com/en-us/library/14h5k7ff(v=vs.71).aspx> [↑](#footnote-ref-47)
48. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa364957(v=VS.85).aspx> [↑](#footnote-ref-48)
49. For more information see <http://msdn.microsoft.com/en-us/library/ms724284(VS.85).aspx> [↑](#footnote-ref-49)
50. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms724320(v=vs.85).aspx> [↑](#footnote-ref-50)
51. For more information see <http://msdn.microsoft.com/en-us/library/ms724284(VS.85).aspx> [↑](#footnote-ref-51)
52. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms724320(v=vs.85).aspx> [↑](#footnote-ref-52)
53. For more information see <http://msdn.microsoft.com/en-us/library/ms724284(VS.85).aspx> [↑](#footnote-ref-53)
54. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms724320(v=vs.85).aspx> [↑](#footnote-ref-54)
55. For more information see <http://msdn.microsoft.com/en-us/library/ms680355(VS.85).aspx> [↑](#footnote-ref-55)
56. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464(v=vs.85).aspx> [↑](#footnote-ref-56)
57. For more information see <http://msdn.microsoft.com/en-us/library/system.diagnostics.fileversioninfo.aspx> [↑](#footnote-ref-57)
58. For more information see <http://msdn.microsoft.com/en-us/library/aa364960(VS.85).aspx> [↑](#footnote-ref-58)
59. For more information see <http://msdn.microsoft.com/en-us/library/aa364946(VS.85).aspx> [↑](#footnote-ref-59)
60. For more information see <http://support.microsoft.com/kb/824994> [↑](#footnote-ref-60)
61. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464(v=vs.85).aspx> [↑](#footnote-ref-61)
62. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464(v=vs.85).aspx> [↑](#footnote-ref-62)
63. For more information see <http://msdn.microsoft.com/en-us/library/system.diagnostics.fileversioninfo.aspx> [↑](#footnote-ref-63)
64. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464(v=vs.85).aspx> [↑](#footnote-ref-64)
65. For more information see <http://msdn.microsoft.com/en-us/library/system.diagnostics.fileversioninfo.aspx> [↑](#footnote-ref-65)
66. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464(v=vs.85).aspx> [↑](#footnote-ref-66)
67. For more information see <http://msdn.microsoft.com/en-us/library/system.diagnostics.fileversioninfo.aspx> [↑](#footnote-ref-67)
68. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464(v=vs.85).aspx> [↑](#footnote-ref-68)
69. For more information see <http://msdn.microsoft.com/en-us/library/system.diagnostics.fileversioninfo.aspx> [↑](#footnote-ref-69)
70. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464(v=vs.85).aspx> [↑](#footnote-ref-70)
71. For more information see <http://msdn.microsoft.com/en-us/library/system.diagnostics.fileversioninfo.aspx> [↑](#footnote-ref-71)
72. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464(v=vs.85).aspx> [↑](#footnote-ref-72)
73. For more information see <http://msdn.microsoft.com/en-us/library/system.diagnostics.fileversioninfo.aspx> [↑](#footnote-ref-73)
74. For more information see <http://msdn.microsoft.com/en-us/library/aa384187(v=vs.85).aspx> [↑](#footnote-ref-74)
75. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms724182(v=VS.85).aspx> [↑](#footnote-ref-75)
76. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms724836(v=vs.85).aspx> [↑](#footnote-ref-76)
77. For more information see <http://msdn.microsoft.com/en-us/library/aa384187(v=vs.85).aspx> [↑](#footnote-ref-77)
78. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms724836(v=vs.85).aspx> [↑](#footnote-ref-78)
79. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms724911(v=vs.85).aspx> [↑](#footnote-ref-79)
80. For more information see <http://msdn.microsoft.com/en-us/library/ms724284(VS.85).aspx> [↑](#footnote-ref-80)
81. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms724902(v=vs.85).aspx> [↑](#footnote-ref-81)
82. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms724911(v=vs.85).aspx> [↑](#footnote-ref-82)
83. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms724911(v=vs.85).aspx> [↑](#footnote-ref-83)
84. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms724072(v=VS.85).aspx> [↑](#footnote-ref-84)
85. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms724836(v=vs.85).aspx> [↑](#footnote-ref-85)
86. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms724911(v=vs.85).aspx> [↑](#footnote-ref-86)
87. For more information see <http://msdn.microsoft.com/en-us/library/ms724284(VS.85).aspx> [↑](#footnote-ref-87)
88. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms724902(v=vs.85).aspx> [↑](#footnote-ref-88)
89. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms724911(v=vs.85).aspx> [↑](#footnote-ref-89)
90. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms724911(v=vs.85).aspx> [↑](#footnote-ref-90)
91. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms724072(v=VS.85).aspx> [↑](#footnote-ref-91)
92. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms724836(v=vs.85).aspx> [↑](#footnote-ref-92)
93. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms724836(v=vs.85).aspx> [↑](#footnote-ref-93)
94. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms724836(v=vs.85).aspx> [↑](#footnote-ref-94)
95. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms724884(v=vs.85).aspx> [↑](#footnote-ref-95)
96. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms724884(v=vs.85).aspx> [↑](#footnote-ref-96)
97. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa364399(v=vs.85).aspx> , <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx>, and <http://technet.microsoft.com/en-us/library/bb727008.aspx> [↑](#footnote-ref-97)
98. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379571(v=vs.85).aspx> [↑](#footnote-ref-98)
99. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa365247(v=vs.85).aspx#paths> [↑](#footnote-ref-99)
100. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa365247(v=vs.85).aspx#paths> [↑](#footnote-ref-100)
101. For more information see <http://msdn.microsoft.com/en-us/library/aa365247.aspx> [↑](#footnote-ref-101)
102. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379166(v=vs.85).aspx> [↑](#footnote-ref-102)
103. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa446645(v=vs.85).aspx> [↑](#footnote-ref-103)
104. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa365247(v=vs.85).aspx#paths> [↑](#footnote-ref-104)
105. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa365247(v=vs.85).aspx#paths> [↑](#footnote-ref-105)
106. For more information see <http://msdn.microsoft.com/en-us/library/aa365247.aspx> [↑](#footnote-ref-106)
107. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379166(v=vs.85).aspx> [↑](#footnote-ref-107)
108. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx> [↑](#footnote-ref-108)
109. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx> [↑](#footnote-ref-109)
110. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx> [↑](#footnote-ref-110)
111. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx> [↑](#footnote-ref-111)
112. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx> [↑](#footnote-ref-112)
113. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx> [↑](#footnote-ref-113)
114. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632(v=VS.85).aspx> [↑](#footnote-ref-114)
115. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632(v=VS.85).aspx> [↑](#footnote-ref-115)
116. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632(v=VS.85).aspx> [↑](#footnote-ref-116)
117. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632(v=VS.85).aspx> [↑](#footnote-ref-117)
118. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116(v=vs.85).aspx> [↑](#footnote-ref-118)
119. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116(v=vs.85).aspx> [↑](#footnote-ref-119)
120. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116(v=vs.85).aspx> [↑](#footnote-ref-120)
121. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116(v=vs.85).aspx> [↑](#footnote-ref-121)
122. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116(v=vs.85).aspx> [↑](#footnote-ref-122)
123. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116(v=vs.85).aspx> [↑](#footnote-ref-123)
124. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116(v=vs.85).aspx> [↑](#footnote-ref-124)
125. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116(v=vs.85).aspx> [↑](#footnote-ref-125)
126. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116(v=vs.85).aspx> [↑](#footnote-ref-126)
127. For more information see <http://msdn.microsoft.com/en-us/library/aa384187(v=vs.85).aspx> [↑](#footnote-ref-127)
128. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa365247(v=vs.85).aspx#paths> [↑](#footnote-ref-128)
129. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa365247(v=vs.85).aspx#paths> [↑](#footnote-ref-129)
130. For more information see <http://msdn.microsoft.com/en-us/library/aa365247.aspx> [↑](#footnote-ref-130)
131. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379166(v=vs.85).aspx> [↑](#footnote-ref-131)
132. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx> [↑](#footnote-ref-132)
133. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx> [↑](#footnote-ref-133)
134. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx> [↑](#footnote-ref-134)
135. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx> [↑](#footnote-ref-135)
136. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx> [↑](#footnote-ref-136)
137. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx> [↑](#footnote-ref-137)
138. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632(v=VS.85).aspx> [↑](#footnote-ref-138)
139. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632(v=VS.85).aspx> [↑](#footnote-ref-139)
140. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632(v=VS.85).aspx> [↑](#footnote-ref-140)
141. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632(v=VS.85).aspx> [↑](#footnote-ref-141)
142. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116(v=vs.85).aspx> [↑](#footnote-ref-142)
143. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116(v=vs.85).aspx> [↑](#footnote-ref-143)
144. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116(v=vs.85).aspx> [↑](#footnote-ref-144)
145. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116(v=vs.85).aspx> [↑](#footnote-ref-145)
146. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116(v=vs.85).aspx> [↑](#footnote-ref-146)
147. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116(v=vs.85).aspx> [↑](#footnote-ref-147)
148. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116(v=vs.85).aspx> [↑](#footnote-ref-148)
149. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116(v=vs.85).aspx> [↑](#footnote-ref-149)
150. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116(v=vs.85).aspx> [↑](#footnote-ref-150)
151. For more information see <http://msdn.microsoft.com/en-us/library/aa384187(v=vs.85).aspx> [↑](#footnote-ref-151)
152. For more information see <http://msdn.microsoft.com/en-us/library/cc244650(v=PROT.10).aspx> [↑](#footnote-ref-152)
153. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379571(v=vs.85).aspx> [↑](#footnote-ref-153)
154. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379166(v=vs.85).aspx> [↑](#footnote-ref-154)
155. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379166(v=vs.85).aspx> [↑](#footnote-ref-155)
156. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx> [↑](#footnote-ref-156)
157. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx> [↑](#footnote-ref-157)
158. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx> [↑](#footnote-ref-158)
159. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx> [↑](#footnote-ref-159)
160. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx> [↑](#footnote-ref-160)
161. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx> [↑](#footnote-ref-161)
162. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632(v=VS.85).aspx> [↑](#footnote-ref-162)
163. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632(v=VS.85).aspx> [↑](#footnote-ref-163)
164. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632(v=VS.85).aspx> [↑](#footnote-ref-164)
165. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632(v=VS.85).aspx> [↑](#footnote-ref-165)
166. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/dd162751(v=vs.85).aspx> [↑](#footnote-ref-166)
167. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/dd145082(v=vs.85).aspx> [↑](#footnote-ref-167)
168. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/dd162751(v=vs.85).aspx> [↑](#footnote-ref-168)
169. For more information see <http://msdn.microsoft.com/en-us/library/cc244650(v=PROT.10).aspx> [↑](#footnote-ref-169)
170. For more information see <http://msdn.microsoft.com/en-us/library/cc244650(v=PROT.10).aspx> [↑](#footnote-ref-170)
171. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379166(v=vs.85).aspx> [↑](#footnote-ref-171)
172. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx> [↑](#footnote-ref-172)
173. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx> [↑](#footnote-ref-173)
174. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx> [↑](#footnote-ref-174)
175. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx> [↑](#footnote-ref-175)
176. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx> [↑](#footnote-ref-176)
177. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx> [↑](#footnote-ref-177)
178. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632(v=VS.85).aspx> [↑](#footnote-ref-178)
179. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632(v=VS.85).aspx> [↑](#footnote-ref-179)
180. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632(v=VS.85).aspx> [↑](#footnote-ref-180)
181. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632(v=VS.85).aspx> [↑](#footnote-ref-181)
182. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/dd162751(v=vs.85).aspx> [↑](#footnote-ref-182)
183. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/dd145082(v=vs.85).aspx> [↑](#footnote-ref-183)
184. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/dd162751(v=vs.85).aspx> [↑](#footnote-ref-184)
185. For more information see <http://msdn.microsoft.com/en-us/library/cc244650(v=PROT.10).aspx> [↑](#footnote-ref-185)
186. For more information see <http://msdn.microsoft.com/en-us/library/cc244650(v=PROT.10).aspx> [↑](#footnote-ref-186)
187. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa374909(v=vs.85).aspx> [↑](#footnote-ref-187)
188. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms677942(v=vs.85).aspx> [↑](#footnote-ref-188)
189. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/bb530716(v=vs.85).aspx> [↑](#footnote-ref-189)
190. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/bb530716(v=vs.85).aspx> [↑](#footnote-ref-190)
191. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/bb545671(v=VS.85).aspx> [↑](#footnote-ref-191)
192. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/bb530716(v=vs.85).aspx> [↑](#footnote-ref-192)
193. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/bb530716(v=vs.85).aspx> [↑](#footnote-ref-193)
194. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/bb545671(v=VS.85).aspx> [↑](#footnote-ref-194)
195. For more information see <http://technet.microsoft.com/en-us/library/cc766468(WS.10).aspx> [↑](#footnote-ref-195)
196. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms721903(v=vs.85).aspx> [↑](#footnote-ref-196)
197. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms721903(v=vs.85).aspx> [↑](#footnote-ref-197)
198. For more information see <http://msdn.microsoft.com/en-us/library/dd976913(v=PROT.10).aspx> [↑](#footnote-ref-198)
199. For more information see <http://msdn.microsoft.com/en-us/library/dd973928(v=PROT.10).aspx> [↑](#footnote-ref-199)
200. For more information see <http://technet.microsoft.com/en-us/library/cc766468(WS.10).aspx> [↑](#footnote-ref-200)
201. For more information see <http://msdn.microsoft.com/en-us/library/0e57a2df-f576-4f59-8c6e-9515567f9900(v=PROT.10)#ad_ds> [↑](#footnote-ref-201)
202. For more information see <http://msdn.microsoft.com/en-us/library/dd973928(v=PROT.10).aspx> [↑](#footnote-ref-202)
203. For more information see <http://technet.microsoft.com/en-us/library/cc766468(WS.10).aspx> [↑](#footnote-ref-203)
204. For more information see <http://msdn.microsoft.com/en-us/library/0e57a2df-f576-4f59-8c6e-9515567f9900(v=PROT.10)#ad_ds> [↑](#footnote-ref-204)
205. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms721882(v=vs.85).aspx> [↑](#footnote-ref-205)
206. For more information see <http://msdn.microsoft.com/en-us/library/ms878685.aspx> [↑](#footnote-ref-206)
207. For more information see line 110 of <http://doxygen.reactos.org/da/d6c/lmaccess_8h_source.html> [↑](#footnote-ref-207)
208. For more information see <http://msdn.microsoft.com/en-us/library/ms878685.aspx> [↑](#footnote-ref-208)
209. For more information see line 110 of <http://doxygen.reactos.org/da/d6c/lmaccess_8h_source.html> [↑](#footnote-ref-209)
210. For more information about the various tools for lockout policies see <http://technet.microsoft.com/en-us/library/cc738772(WS.10).aspx>

     For more information about lockout policies in general see <http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=6218> [↑](#footnote-ref-210)
211. For more information about the various tools for lockout policies see <http://technet.microsoft.com/en-us/library/cc738772(WS.10).aspx>

     For more information about lockout policies in general see <http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=6218> [↑](#footnote-ref-211)
212. For more information about the various tools for lockout policies see <http://technet.microsoft.com/en-us/library/cc738772(WS.10).aspx>

     For more information about lockout policies in general see <http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=6218> [↑](#footnote-ref-212)
213. For more information about the properties in lockoutpolicy\_state see <http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=6218> [↑](#footnote-ref-213)
214. For more information see line 110 of <http://doxygen.reactos.org/da/d6c/lmaccess_8h_source.html> [↑](#footnote-ref-214)
215. For more information see the "NetUserModalsSet anomalies" comment under Community Additions in

     <http://msdn.microsoft.com/en-us/library/windows/desktop/aa371355(v=vs.85).aspx> [↑](#footnote-ref-215)
216. For more information see the "NetUserModalsSet anomalies" comment under Community Additions in

     <http://msdn.microsoft.com/en-us/library/windows/desktop/aa371355(v=vs.85).aspx> [↑](#footnote-ref-216)
217. For more information see

     <http://msdn.microsoft.com/en-us/library/windows/desktop/aa394582%28v=vs.85%29.aspx> [↑](#footnote-ref-217)
218. For more information see

     <http://msdn.microsoft.com/en-us/library/windows/desktop/aa394582%28v=vs.85%29.aspx> [↑](#footnote-ref-218)
219. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa394582%28v=vs.85%29.aspx> [↑](#footnote-ref-219)
220. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa394606%28v=vs.85%29.aspx> [↑](#footnote-ref-220)
221. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa394582%28v=vs.85%29.aspx> [↑](#footnote-ref-221)
222. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa394582%28v=vs.85%29.aspx> [↑](#footnote-ref-222)
223. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa394606%28v=vs.85%29.aspx> [↑](#footnote-ref-223)
224. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa394582%28v=vs.85%29.aspx> [↑](#footnote-ref-224)
225. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa394606%28v=vs.85%29.aspx> [↑](#footnote-ref-225)
226. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379637(v=vs.85).aspx> [↑](#footnote-ref-226)
227. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379571%28v=vs.85%29.aspx> [↑](#footnote-ref-227)
228. For more information about trustees see

     <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379637(v=vs.85).aspx>

     For more information about SIDs see

     <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379571%28v=vs.85%29.aspx> [↑](#footnote-ref-228)
229. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379637(v=vs.85).aspx> [↑](#footnote-ref-229)
230. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379159%28v=VS.85%29.aspx> [↑](#footnote-ref-230)
231. For more information about trustees see

     <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379637(v=vs.85).aspx>

     For more information about SIDs see

     <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379571%28v=vs.85%29.aspx> [↑](#footnote-ref-231)
232. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379637(v=vs.85).aspx> [↑](#footnote-ref-232)
233. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379159%28v=VS.85%29.aspx> [↑](#footnote-ref-233)
234. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379637(v=vs.85).aspx> [↑](#footnote-ref-234)
235. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379159%28v=VS.85%29.aspx> [↑](#footnote-ref-235)
236. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379637(v=vs.85).aspx> [↑](#footnote-ref-236)
237. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379571%28v=vs.85%29.aspx> [↑](#footnote-ref-237)
238. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379166(v=vs.85).aspx> [↑](#footnote-ref-238)
239. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379637(v=vs.85).aspx> [↑](#footnote-ref-239)
240. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379159%28v=VS.85%29.aspx> [↑](#footnote-ref-240)
241. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379637(v=vs.85).aspx> [↑](#footnote-ref-241)
242. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379159%28v=VS.85%29.aspx> [↑](#footnote-ref-242)
243. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms714395(v=vs.85).aspx> [↑](#footnote-ref-243)
244. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms714395(v=vs.85).aspx> [↑](#footnote-ref-244)
245. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ee706608(v=vs.85).aspx> [↑](#footnote-ref-245)
246. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms714423(v=vs.85).aspx> [↑](#footnote-ref-246)
247. For more information see <http://msdn.microsoft.com/en-us/library/system.management.automation.pslanguagemode.aspx> [↑](#footnote-ref-247)
248. For more information see <http://www.microsoft.com/download/en/details.aspx?id=9706> [↑](#footnote-ref-248)
249. For more information see <http://technet.microsoft.com/en-us/library/dd819471.aspx> [↑](#footnote-ref-249)
250. For more information see the examples in <http://technet.microsoft.com/en-us/library/dd819471.aspx> [↑](#footnote-ref-250)
251. For more information see the examples in <http://technet.microsoft.com/en-us/library/dd819471.aspx> [↑](#footnote-ref-251)
252. For more information see <http://www.microsoft.com/download/en/details.aspx?id=9706> [↑](#footnote-ref-252)
253. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms714428(v=vs.85).aspx> [↑](#footnote-ref-253)
254. For more information see <http://www.microsoft.com/download/en/details.aspx?id=9706> [↑](#footnote-ref-254)
255. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms714423(v=vs.85).aspx> [↑](#footnote-ref-255)
256. For more information see <http://www.microsoft.com/download/en/details.aspx?id=9706> [↑](#footnote-ref-256)
257. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/dd878238(v=vs.85).aspx#RD03> [↑](#footnote-ref-257)
258. For more information see <http://technet.microsoft.com/en-us/library/dd315291.aspx> [↑](#footnote-ref-258)
259. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms714395(v=vs.85).aspx> [↑](#footnote-ref-259)
260. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms714423(v=vs.85).aspx> [↑](#footnote-ref-260)
261. For more information see <http://www.microsoft.com/download/en/details.aspx?id=9706> [↑](#footnote-ref-261)
262. For more information see <http://technet.microsoft.com/en-us/library/dd819471.aspx> [↑](#footnote-ref-262)
263. For more information see the examples in <http://technet.microsoft.com/en-us/library/dd819471.aspx> [↑](#footnote-ref-263)
264. For more information see the examples in <http://technet.microsoft.com/en-us/library/dd819471.aspx> [↑](#footnote-ref-264)
265. For more information see <http://www.microsoft.com/download/en/details.aspx?id=9706> [↑](#footnote-ref-265)
266. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms714428(v=vs.85).aspx> [↑](#footnote-ref-266)
267. For more information see <http://www.microsoft.com/download/en/details.aspx?id=9706> [↑](#footnote-ref-267)
268. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms714423(v=vs.85).aspx> [↑](#footnote-ref-268)
269. For more information see <http://www.microsoft.com/download/en/details.aspx?id=9706> [↑](#footnote-ref-269)
270. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/dd878238(v=vs.85).aspx#RD03> [↑](#footnote-ref-270)
271. For more information see <http://technet.microsoft.com/en-us/library/dd315291.aspx> [↑](#footnote-ref-271)
272. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms714395(v=vs.85).aspx> [↑](#footnote-ref-272)
273. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms714423(v=vs.85).aspx> [↑](#footnote-ref-273)
274. For more information see <http://www.microsoft.com/download/en/details.aspx?id=9706> [↑](#footnote-ref-274)
275. For more information see <http://technet.microsoft.com/en-us/library/dd819471.aspx> [↑](#footnote-ref-275)
276. For more information see the examples in <http://technet.microsoft.com/en-us/library/dd819471.aspx> [↑](#footnote-ref-276)
277. For more information see the examples in <http://technet.microsoft.com/en-us/library/dd819471.aspx> [↑](#footnote-ref-277)
278. For more information see <http://www.microsoft.com/download/en/details.aspx?id=9706> [↑](#footnote-ref-278)
279. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms714428(v=vs.85).aspx> [↑](#footnote-ref-279)
280. For more information see <http://www.microsoft.com/download/en/details.aspx?id=9706> [↑](#footnote-ref-280)
281. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms714423(v=vs.85).aspx> [↑](#footnote-ref-281)
282. For more information see <http://www.microsoft.com/download/en/details.aspx?id=9706> [↑](#footnote-ref-282)
283. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/dd878238(v=vs.85).aspx#RD03> [↑](#footnote-ref-283)
284. For more information see <http://technet.microsoft.com/en-us/library/dd315291.aspx> [↑](#footnote-ref-284)
285. For more information see <http://technet.microsoft.com/en-us/library/bb726978.aspx> [↑](#footnote-ref-285)
286. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa370653(v=vs.85).aspx> [↑](#footnote-ref-286)
287. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa370653(v=vs.85).aspx> [↑](#footnote-ref-287)
288. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa370653(v=vs.85).aspx> [↑](#footnote-ref-288)
289. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa370653(v=vs.85).aspx> [↑](#footnote-ref-289)
290. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa370653(v=vs.85).aspx> [↑](#footnote-ref-290)
291. For more information see <http://technet.microsoft.com/en-us/library/bb726978.aspx> [↑](#footnote-ref-291)
292. For more information see

     <http://msdn.microsoft.com/en-us/library/windows/desktop/aa394582%28v=vs.85%29.aspx> [↑](#footnote-ref-292)
293. For more information see

     <http://msdn.microsoft.com/en-us/library/windows/desktop/aa394582%28v=vs.85%29.aspx> [↑](#footnote-ref-293)
294. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa394582%28v=vs.85%29.aspx> [↑](#footnote-ref-294)
295. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa394606%28v=vs.85%29.aspx> [↑](#footnote-ref-295)
296. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa394582%28v=vs.85%29.aspx> [↑](#footnote-ref-296)
297. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa394582%28v=vs.85%29.aspx> [↑](#footnote-ref-297)
298. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa394606%28v=vs.85%29.aspx> [↑](#footnote-ref-298)
299. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa394582%28v=vs.85%29.aspx> [↑](#footnote-ref-299)
300. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa394606%28v=vs.85%29.aspx> [↑](#footnote-ref-300)
301. For more information see <http://technet.microsoft.com/en-us/library/cc739393(WS.10).aspx> [↑](#footnote-ref-301)
302. For more information about SID\_NAME\_TYPE see <http://msdn.microsoft.com/en-us/library/windows/hardware/ff556744(v=vs.85).aspx>

     For more information about LookupAccountSid, see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379166(v=vs.85).aspx> [↑](#footnote-ref-302)
303. For more information see the remarks section of

     <http://msdn.microsoft.com/en-us/library/windows/desktop/aa370653(v=vs.85).aspx> [↑](#footnote-ref-303)
304. For more information see the remarks section of

     <http://msdn.microsoft.com/en-us/library/windows/desktop/aa370653(v=vs.85).aspx> [↑](#footnote-ref-304)
305. For more information see the Remarks section of <http://msdn.microsoft.com/en-us/library/windows/desktop/aa370653(v=vs.85).aspx> [↑](#footnote-ref-305)
306. For more information see the Remarks section of <http://msdn.microsoft.com/en-us/library/windows/desktop/aa370653(v=vs.85).aspx> [↑](#footnote-ref-306)
307. For more information see the remarks section of

     <http://msdn.microsoft.com/en-us/library/windows/desktop/aa370653(v=vs.85).aspx> [↑](#footnote-ref-307)
308. For more information see the remarks section of

     <http://msdn.microsoft.com/en-us/library/windows/desktop/aa370653(v=vs.85).aspx> [↑](#footnote-ref-308)
309. For more information see the remarks section of

     <http://msdn.microsoft.com/en-us/library/windows/desktop/aa370653(v=vs.85).aspx> [↑](#footnote-ref-309)
310. For more information about SID\_NAME\_TYPE see <http://msdn.microsoft.com/en-us/library/windows/hardware/ff556744(v=vs.85).aspx>

     For more information about LookupAccountSid, see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379166(v=vs.85).aspx> [↑](#footnote-ref-310)
311. For more information see <http://technet.microsoft.com/en-us/query/ms524661> [↑](#footnote-ref-311)
312. For more information see <http://support.microsoft.com/kb/240941> [↑](#footnote-ref-312)
313. For more information see <http://support.microsoft.com/kb/240941> [↑](#footnote-ref-313)
314. For more information see Metabase Concepts in <http://technet.microsoft.com/en-us/query/ms524661> [↑](#footnote-ref-314)
315. For more information see Internal ID in <http://msdn.microsoft.com/en-us/library/ms524578(v=vs.90).aspx#id> [↑](#footnote-ref-315)
316. For more information see <http://msdn.microsoft.com/en-us/library/cc233554(v=PROT.10).aspx> [↑](#footnote-ref-316)
317. For more information see <http://msdn.microsoft.com/en-us/library/cc233554(v=PROT.10).aspx> [↑](#footnote-ref-317)
318. For more information see Metabase Concepts in <http://technet.microsoft.com/en-us/query/ms524661> [↑](#footnote-ref-318)
319. For more information see Internal ID in <http://msdn.microsoft.com/en-us/library/ms524578(v=vs.90).aspx#id> [↑](#footnote-ref-319)
320. For more information see <http://msdn.microsoft.com/en-us/library/ms524635(v=VS.90).aspx> [↑](#footnote-ref-320)
321. For more information see <http://msdn.microsoft.com/en-us/library/ms524635(v=VS.90).aspx> [↑](#footnote-ref-321)
322. For more information see Property Attributes in <http://msdn.microsoft.com/en-us/library/ms524578(v=vs.90).aspx> [↑](#footnote-ref-322)
323. For more information see <http://msdn.microsoft.com/en-us/library/ms524951(v=vs.90).aspx> [↑](#footnote-ref-323)
324. For more information see <http://msdn.microsoft.com/en-us/library/cc233554(v=PROT.10).aspx> [↑](#footnote-ref-324)
325. For more information see Metabase Concepts in <http://technet.microsoft.com/en-us/query/ms524661> [↑](#footnote-ref-325)
326. For more information see Internal ID in <http://msdn.microsoft.com/en-us/library/ms524578(v=vs.90).aspx#id> [↑](#footnote-ref-326)
327. For more information see <http://msdn.microsoft.com/en-us/library/ms524635(v=VS.90).aspx> [↑](#footnote-ref-327)
328. For more information see <http://msdn.microsoft.com/en-us/library/ms524635(v=VS.90).aspx> [↑](#footnote-ref-328)
329. For more information see Property Attributes in <http://msdn.microsoft.com/en-us/library/ms524578(v=vs.90).aspx> [↑](#footnote-ref-329)
330. For more information see <http://msdn.microsoft.com/en-us/library/ms524951(v=vs.90).aspx> [↑](#footnote-ref-330)
331. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms681917(v=VS.85).aspx> [↑](#footnote-ref-331)
332. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa394372(v=vs.85).aspx> [↑](#footnote-ref-332)
333. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms681917(v=VS.85).aspx> [↑](#footnote-ref-333)
334. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa394372(v=vs.85).aspx> [↑](#footnote-ref-334)
335. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/ms681917(v=VS.85).aspx> [↑](#footnote-ref-335)
336. For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa394372(v=vs.85).aspx> [↑](#footnote-ref-336)