

THE MITRE CORPORATION

The OVAL® Language Windows Component Model Specification

Version 5.11

Danny Haynes, Stelios Melachrinoudis

12/18/2014

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 DAMAGES¹.

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 or directly to the OVAL Moderator at oval@mitre.org².

¹ For more information see <https://oval.mitre.org/about/termsofuse.html>

² For more information see <https://oval.mitre.org/>

Contents

Acknowledgements.....	1
Trademark Information.....	1
Warnings	1
Feedback	1
1. Introduction	6
1.1 Document Conventions	6
1.2 Document Structure.....	7
2. OVAL Language Windows Component Model.....	8
2.1 Data Model Conventions	8
2.2 win-def:file_test.....	8
2.2.1 Known Supported Platforms.....	8
2.3 win-def:file_object.....	9
2.4 win-def:FileBehaviors	11
2.5 win-def:file_state.....	12
2.6 win-sc:file_item.....	19
2.7 win-def:EntityStateFileTypeType	27
2.8 win-sc:EntityItemFileTypeType	27
2.12. win-def:EntityStateWindowsViewType	27
2.13. win-sc:EntityItemWindowsViewType	28
2.14. win-def:registry_test.....	29
2.14.1. Known Supported Platforms.....	29
2.15. win-def:registry_object.....	29
2.16. win-def:RegistryBehaviors	32
2.17. win-def:registry_state.....	34
2.18. win-sc:registry_item	37
2.19. win-def:EntityObjectRegistryHiveType	40
2.20. win-def:EntityStateRegistryHiveType	40
2.21. win-sc:EntityItemRegistryHiveType	40

2.22.	win-def:EntityStateRegistryTypeType.....	41
2.23.	win-sc:EntityItemRegistryTypeType.....	41
2.24.	win-def:fileeffectiverights53_test.....	42
2.24.1.	Known Supported Platforms.....	43
2.25.	win-def:fileeffectiverights53_object.....	43
2.26.	FileEffectiveRights53Behaviors.....	46
2.27.	win-def:fileeffectiverights53_state.....	48
2.28.	win-sc:fileeffectiverights53__item.....	53
2.29.	win-def:printereffectiverights_test.....	58
2.29.1.	Known Supported Platforms.....	58
2.30.	win-def:printereffectiverights_object.....	58
2.31.	win-def:PrinterEffectiveRightsBehaviors.....	60
2.32.	win-def:printereffectiverights_state.....	62
2.33.	win-sc:printereffectiverights_item.....	64
2.34.	win-def:accesstoken_test.....	66
2.34.1.	Known Supported Platforms.....	67
2.35.	win-def:accesstoken_object.....	67
2.36.	win-def:AccesstokenBehaviors.....	68
2.37.	win-def:accesstoken_state.....	70
2.38.	win-sc:accesstoken_item.....	76
2.39.	win-def:auditeventpolicy_test.....	82
2.39.1.	Known Supported Platforms.....	83
2.40.	win-def:auditeventpolicy_object.....	83
2.41.	win-def:auditeventpolicy_state.....	83
2.42.	win-sc:auditeventpolicy__item.....	86
2.43.	win-def:EntityStateAuditType.....	88
2.44.	win-sc:EntityItemAuditType.....	88
2.45.	win-def:auditeventpolicysubcategories_test.....	89
2.45.1.	Known Supported Platforms.....	89
2.46.	win-def:auditeventpolicysubcategories_object.....	89
2.47.	win-def: auditeventpolicysubcategories_state.....	90

2.48.	win-sc:auditeventpolicysubcategories__item	101
2.49.	win-def:EntityStateAuditType.....	112
2.50.	win-sc:EntityItemAuditType.....	112
2.51.	win-def:passwordpolicy_test.....	113
2.51.1.	Known Supported Platforms.....	113
2.52.	win-def:passwordpolicy_object.....	113
2.53.	win-def:passwordpolicy_state	114
2.54.	win-sc:passwordpolicy_item.....	117
2.55.	win-def:lockoutpolicy_test	121
2.55.1.	Known Supported Platforms.....	121
2.56.	win-def:lockoutpolicy_object	121
2.57.	win-def: lockoutpolicy_state	122
2.58.	win-sc: lockoutpolicy_item	125
2.59.	win-def:wmi57_test.....	127
2.59.1.	Known Supported Platforms.....	127
2.60.	win-def:wmi57_object.....	127
2.61.	win-def: wmi57_state	129
2.62.	win-sc:wmi57_item.....	130
2.63.	win-def:sid_test	131
2.63.1.	Known Supported Platforms.....	132
2.64.	win-def:sid_object	132
2.65.	win-def:SidBehaviors	134
2.66.	win-def:sid_state	135
2.67.	win-sc:sid_item	137
2.68.	win-def:sid_sid_test.....	138
2.68.1.	Known Supported Platforms.....	139
2.69.	win-def:sid_sid_object.....	139
2.70.	win-def:SidSidBehaviors	140
2.71.	win-def:sid_sid_state.....	141
2.72.	win-sc:sid_sid_item.....	143
2.73.	win-def:cmdlet_test.....	144

2.73.1.	Known Supported Platforms.....	144
2.74.	win-def:cmdlet_object.....	145
2.75.	win-def:cmdlet_state.....	148
2.76.	win-sc:cmdlet_item.....	150
2.77.	win-def:EntityObjectGUIDType.....	153
2.78.	win-def:EntityStateGUIDType.....	153
2.79.	win-sc:EntityItemGUIDType.....	154
2.80.	win-def:EntityObjectCmdletVerbType.....	154
2.81.	win-def:EntityStateCmdletVerbType.....	155
2.82.	win-sc:EntityItemCmdletVerbType.....	156
2.83.	win-def:user_test.....	156
2.83.1.	Known Supported Platforms.....	157
2.84.	win-def:user_object.....	157
2.85.	win-def:user_state.....	159
2.86.	win-sc:user_item.....	161
2.87.	win-def:user_sid55_test.....	164
2.87.1.	Known Supported Platforms.....	164
2.88.	win-def:user_sid55_object.....	165
2.89.	win-def:user_sid55_state.....	165
2.90.	win-sc:user_sid_item.....	167
2.91.	win-def:wmi_test.....	168
2.91.1.	Known Supported Platforms.....	168
2.92.	win-def:wmi_object.....	168
2.93.	win-def:wmi_state.....	170
2.94.	win-sc:wmi_item.....	171
2.95.	win-def:group_test.....	172
2.95.1.	Known Supported Platforms.....	173
2.96.	win-def:group_object.....	173
2.97.	win-def:group_state.....	175
2.98.	win-sc:group_item.....	178
2.99.	win-def:group_sid_test.....	181

2.99.1.	Known Supported Platforms.....	182
2.100.	win-def:group_sid_object.....	182
2.101.	win-def:group_sid_state.....	183
2.102.	win-sc:group_sid_item.....	184
2.103.	win-def:metabase_test.....	186
2.103.1.	Known Supported Platforms.....	186
2.104.	win-def:metabase_object.....	186
2.105.	win-def:metabase_state.....	188
2.106.	win-sc:metabase_item.....	189
2.107.	win-def:process_test.....	191
2.107.1.	Known Supported Platforms.....	191
2.108.	win-def:process_object.....	191
2.109.	win-def:process_state.....	192
2.110.	win-sc:process_item.....	194
Appendix A – Normative References.....		195
Appendix B - Change Log.....		195
Appendix C - Terms and Acronyms.....		196

1. 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 namespaces³ 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:

³ For more information see [http://en.wikipedia.org/wiki/Namespace_\(computer_science\)](http://en.wikipedia.org/wiki/Namespace_(computer_science))

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

2. OVAL Language Windows Component Model

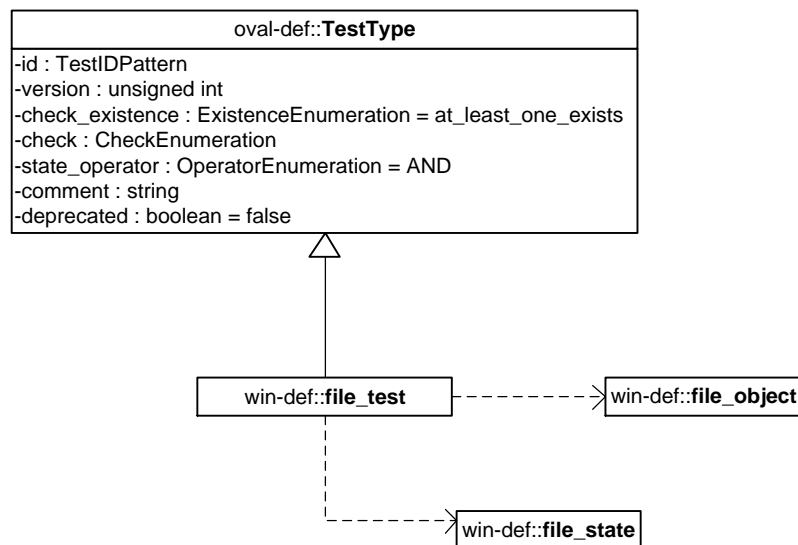
The OVAL Language Windows Component Data Model is the platform-specific extension of the OVAL Language Data Model for Microsoft Windows operating systems.

2.1 Data Model Conventions

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

2.2 win-def:file_test

The `file_test` is used to make assertions about the system state information associated with the directories and files⁴ on file systems supported by Microsoft Windows operating systems. The `file_test` MUST reference one `file_object` and zero or more `file_states`.



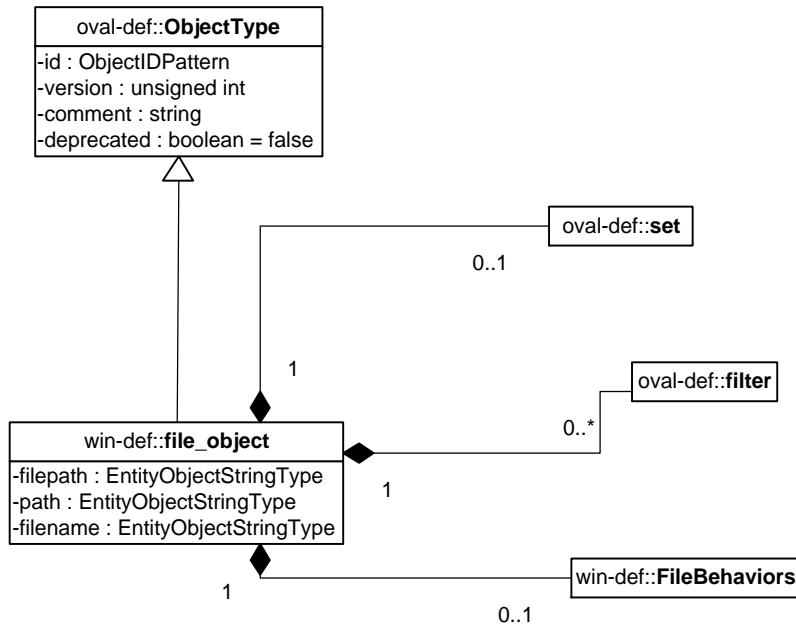
2.2.1 Known Supported Platforms

- Windows XP
- Windows Vista
- Windows 7

⁴ For more information see [http://msdn.microsoft.com/en-us/library/aa364407\(v=VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa364407(v=VS.85).aspx)

2.3 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	Nullable	Description
set	oval-def:set	0..1	false	Enables the expression of complex <code>file_objects</code> that are the result of logically combining and filtering the <code>file_items</code> that are identified by one or more <code>file_objects</code> . 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 <code>file_object</code> collects <code>file_items</code> from the system.
filepath	oval-def:	0..1	false	The absolute path to a file on the system.

	EntityObjectStringType			<p>The absolute path SHOULD align with the guidance provided in the MSDN documentation⁵.</p> <p>A directory MUST NOT be specified for this property.</p> <p>The path and filename properties MUST NOT be specified when this property is specified.</p> <p>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.</p>
path	oval-def: EntityObjectStringType	0..1	false	<p>The directory component of the absolute path to a directory or file on the system.</p> <p>The path component SHOULD align with the guidance provided in the MSDN documentation⁶.</p> <p>The filepath property MUST NOT be specified when this property is specified.</p>
filename	oval-def: EntityObjectStringType	0..1	true	<p>The name of a file to evaluate.</p> <p>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 above⁷.</p> <p>The filepath property MUST NOT be specified when this property is specified.</p> <p>xsi:nil="true" indicates that the <code>file_object</code> MUST collect the set of directories specified by the path entity. In addition, a value for the filename entity</p>

⁵ For more information see <http://msdn.microsoft.com/en-us/library/aa365247.aspx>

⁶ For more information see <http://msdn.microsoft.com/en-us/library/aa365247.aspx>

⁷ For more information see <http://msdn.microsoft.com/en-us/library/aa365247.aspx>

				MUST NOT be specified.
Filter	oval-def:filter	0..*	false	Allows for the explicit inclusion or exclusion of <code>file_items</code> from the set of <code>file_items</code> collected by a <code>file_object</code> . Please see the OVAL Language Specification [2] for additional information.

2.4 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.

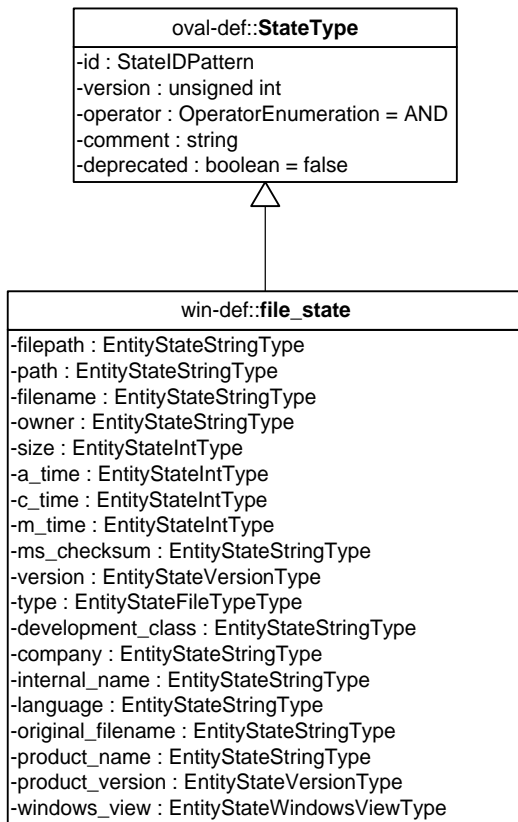
Attribute	Type	Possible Values	Description
max_depth	integer	< -1 -1 0 > 0	Defines the maximum depth of file system traversal when the <code>recurse_direction</code> behavior is set to a value other than <code>'none'</code> . < -1: not permitted. -1: traverse the file system with no limitation. 0: do not traverse the file system. > 0: traverse the file system for the specified number of levels. Default Value: -1
recurse_direction	string	<code>'none'</code> <code>'up'</code> <code>'down'</code>	Defines the direction to recursively visit the directories on the file system. <code>'none'</code> : do not traverse the file system. <code>'up'</code> : traverse the file system by recursively visiting the parent directories. <code>'down'</code> : traverse the file system by recursively visiting the child directories.

			<p>An error MUST NOT be reported when the <code>max_depth</code> behavior specifies a certain level of traversal and that level does not exist.</p> <p>Default Value: none</p>
recurse_file_system	string	<p><i>'all'</i></p> <p><i>'local'</i></p> <p><i>'defined'</i></p>	<p>Defines the file system limitation of any searching. This applies to all operations as specified in the path or filepath entity.</p> <p><i>'all'</i>: traverse both local and remote file systems.</p> <p><i>'local'</i>: only traverse the local file systems.</p> <p><i>'defined'</i>: only traverse the specified file system.</p> <p>The value of <i>'defined'</i> MUST only be used in conjunction with the equality operation because the path or filepath entity must explicitly define a file system.</p> <p>Default Value: all</p>
windows_view	string	<p><i>'32_bit'</i></p> <p><i>'64_bit'</i></p>	<p>64-bit versions of Windows provide an alternate file system view to 32-bit applications⁸. This behavior defines which view should be examined by the <code>file_object</code>.</p> <p><i>'32_bit'</i>: check the 32_bit view of the file system.</p> <p><i>'64_bit'</i>: check the 64_bit view of the file system.</p> <p>This behavior only applies to 64-bit versions of Windows and MUST NOT be applied on other platforms.</p> <p>Default Value: 64-bit</p>

2.5 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.

⁸ For more information see [http://msdn.microsoft.com/en-us/library/aa384187\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/aa384187(v=vs.85).aspx)



Property	Type	Multiplicity	Nullable	Description
filepath	oval-def:EntityStateStringType	0..1	false	<p>The absolute path to a file on the system.</p> <p>The absolute path SHOULD align with the guidance provided in the MSDN documentation⁹.</p> <p>A directory MUST NOT be specified for this property.</p> <p>The max_depth and recurse_direction behaviors MUST NOT be used in conjunction with this property as</p>

⁹ For more information see <http://msdn.microsoft.com/en-us/library/aa365247.aspx>

				they are reserved for use with the path and filename properties.
Path	oval-def:EntityStateStringType	0..1	false	<p>The directory component of the absolute path to a directory or file on the system.</p> <p>The path component SHOULD align with the guidance provided in the MSDN documentation¹⁰.</p>
filename	oval-def:EntityStateStringType	0..1	false	<p>The name of a file to evaluate.</p> <p>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 above¹¹.</p>
owner	oval-def:EntityStateStringType	0..1	false	<p>The owner of the file.</p> <p>The owner MUST BE expressed in the DOMAIN\username format.</p> <p>The username component of the owner can be retrieved using the GetSecurityInfo function¹² and the</p>

¹⁰ For more information see <http://msdn.microsoft.com/en-us/library/aa365247.aspx>

¹¹ For more information see <http://msdn.microsoft.com/en-us/library/aa365247.aspx>

¹² For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa446654\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa446654(v=vs.85).aspx)

				domain component can be retrieved using the LookupAccountSid function ¹³ .
Size	oval-def:EntityStateIntType	0..1	false	<p>The size of the file in bytes.</p> <p>The size of the file can be retrieved using the _stat function¹⁴ or GetFileSizeEx function¹⁵.</p>
a_time	oval-def:EntityStateIntType	0..1	false	<p>The date and time that the file was last accessed.</p> <p>This is valid on NTFS formatted disk drives, but, not on FAT formatted disk drives.</p> <p>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.</p> <p>The GetFileTime function¹⁷ can retrieve the last accessed time.</p>
c_time	oval-def:EntityStateIntType	0..1	false	The date and time that the file was created.

¹³ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379166\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379166(v=vs.85).aspx)

¹⁴ For more information see [http://msdn.microsoft.com/en-us/library/14h5k7ff\(v=vs.71\).aspx](http://msdn.microsoft.com/en-us/library/14h5k7ff(v=vs.71).aspx)

¹⁵ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa364957\(v=VS.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa364957(v=VS.85).aspx)

¹⁶ For more information see [http://msdn.microsoft.com/en-us/library/ms724284\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ms724284(VS.85).aspx)

¹⁷ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms724320\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms724320(v=vs.85).aspx)

				<p>This is valid on NTFS formatted disk drives, but, not on FAT formatted disk drives.</p> <p>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.</p> <p>The GetFileTime function¹⁹ can retrieve the creation time.</p>
m_time	oval-def:EntityStateIntType	0..1	false	<p>The date and time that the file was last modified.</p> <p>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.</p> <p>The GetFileTime function²¹ can retrieve the last modified time.</p>
ms_checksum	oval-def:EntityStateStringType	0..1	false	<p>The checksum of the file.</p> <p>The checksum MUST</p>

¹⁸ For more information see [http://msdn.microsoft.com/en-us/library/ms724284\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ms724284(VS.85).aspx)

¹⁹ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms724320\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms724320(v=vs.85).aspx)

²⁰ For more information see [http://msdn.microsoft.com/en-us/library/ms724284\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ms724284(VS.85).aspx)

²¹ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms724320\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms724320(v=vs.85).aspx)

				align with the value supplied by Microsoft's MapFileAndChecksum function ²² .
version	oval-def: EntityStateVersionType	0..1	false	The version number of the file. This value can be obtained via the VarQueryValue function ²³ or the FileVersionInfo class ²⁴ .
type	win-def: EntityStateFileTypeType	0..1	false	The type of the file. This value can be obtained using the GetFileType function ²⁵ with the exception of FILE_ATTRIBUTE_DIRECTORY which can be obtained with the GetFileAttributesEx function 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 mmmmm-nnnn

²² For more information see [http://msdn.microsoft.com/en-us/library/ms680355\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ms680355(VS.85).aspx)

²³ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464(v=vs.85).aspx)

²⁴ For more information see <http://msdn.microsoft.com/en-us/library/system.diagnostics.fileversioninfo.aspx>

²⁵ For more information see [http://msdn.microsoft.com/en-us/library/aa364960\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa364960(VS.85).aspx)

²⁶ For more information see [http://msdn.microsoft.com/en-us/library/aa364946\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa364946(VS.85).aspx)

				<p>component of the file version formats²⁷.</p> <p>This value can be obtained via the VarQueryValue function²⁸.</p>
company	oval-def:EntityStateStringType	0..1	false	<p>The name of the company that created the file.</p> <p>This value can be obtained via the VarQueryValue function²⁹ or the FileVersionInfo class³⁰.</p>
internal_name	oval-def:EntityStateStringType	0..1	false	<p>The internal name of the file.</p> <p>This value can be obtained via the VarQueryValue function³¹ or the FileVersionInfo class³².</p>
language	oval-def:EntityStateStringType	0..1	false	<p>The description string for the Microsoft Language Identifier associated with the file.</p> <p>This value can be obtained via the VarQueryValue function³³ or the FileVersionInfo class³⁴.</p>
original_filename	oval-def:EntityStateStringType	0..1	false	<p>The original name of the file when it was created.</p>

²⁷ For more information see <http://support.microsoft.com/kb/824994>

²⁸ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464(v=vs.85).aspx)

²⁹ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464(v=vs.85).aspx)

³⁰ For more information see <http://msdn.microsoft.com/en-us/library/system.diagnostics.fileversioninfo.aspx>

³¹ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464(v=vs.85).aspx)

³² For more information see <http://msdn.microsoft.com/en-us/library/system.diagnostics.fileversioninfo.aspx>

³³ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464(v=vs.85).aspx)

³⁴ For more information see <http://msdn.microsoft.com/en-us/library/system.diagnostics.fileversioninfo.aspx>

				This value can be obtained via the VarQueryValue function ³⁵ or the FileVersionInfo class 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 or the FileVersionInfo class 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 or the FileVersionInfo class ⁴⁰ .
windows_view	win-def: EntityStateWindowsViewType	0..1	false	The targeted file system view ⁴¹ where the file or directory was collected.

2.6 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.

³⁵ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464(v=vs.85).aspx)

³⁶ For more information see <http://msdn.microsoft.com/en-us/library/system.diagnostics.fileversioninfo.aspx>

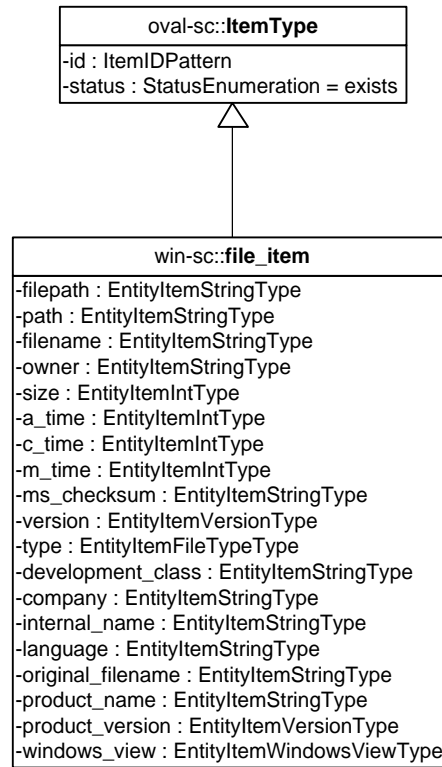
³⁷ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464(v=vs.85).aspx)

³⁸ For more information see <http://msdn.microsoft.com/en-us/library/system.diagnostics.fileversioninfo.aspx>

³⁹ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464(v=vs.85).aspx)

⁴⁰ For more information see <http://msdn.microsoft.com/en-us/library/system.diagnostics.fileversioninfo.aspx>

⁴¹ For more information see [http://msdn.microsoft.com/en-us/library/aa384187\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/aa384187(v=vs.85).aspx)



Property	Type	Multiplicity	Nilable	Description
filepath	oval-sc: EntityItemStringType	0..1	false	<p>The absolute path to a file on the system.</p> <p>The absolute path SHOULD align with the guidance provided in the MSDN documentation⁴².</p> <p>A directory MUST NOT be specified for this property.</p> <p>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.</p>
path	oval-sc:	0..1	false	The directory

⁴² For more information see <http://msdn.microsoft.com/en-us/library/aa365247.aspx>

	EntityItemStringType			<p>component of the absolute path to a directory or file on the system.</p> <p>The path component SHOULD align with the guidance provided in the MSDN documentation⁴³.</p>
filename	oval-sc: EntityItemStringType	0..1	true	<p>The name of a file to evaluate.</p> <p>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 above⁴⁴.</p> <p>xsi:nil="true" MUST be set when the filename entity, in the collecting <code>file_object</code>, has <code>xsi:nil="true"</code> set. In addition, the status of this entity MUST be <i>'not collected'</i> and a value for this entity MUST NOT be specified.</p>
owner	oval-sc: EntityItemStringType	0..1	false	<p>The owner of the file.</p> <p>The owner MUST BE expressed in the DOMAIN\username</p>

⁴³ For more information see <http://msdn.microsoft.com/en-us/library/aa365247.aspx>

⁴⁴ For more information see <http://msdn.microsoft.com/en-us/library/aa365247.aspx>

				<p>format.</p> <p>The username component of the owner can be retrieved using the GetSecurityInfo function⁴⁵ and the domain component can be retrieved using the LookupAccountSid function⁴⁶.</p>
size	oval-sc:EntityItemIntType	0..1	false	<p>The size of the file in bytes.</p> <p>The size of the file can be retrieved using the _stat function⁴⁷ or GetFileSizeEx function⁴⁸.</p>
a_time	oval-sc:EntityItemIntType	0..1	false	<p>The date and time that the file was last accessed.</p> <p>This is valid on NTFS formatted disk drives, but, not on FAT formatted disk drives.</p> <p>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.</p>

⁴⁵ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa446654\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa446654(v=vs.85).aspx)

⁴⁶ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379166\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379166(v=vs.85).aspx)

⁴⁷ For more information see [http://msdn.microsoft.com/en-us/library/14h5k7ff\(v=vs.71\).aspx](http://msdn.microsoft.com/en-us/library/14h5k7ff(v=vs.71).aspx)

⁴⁸ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa364957\(v=VS.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa364957(v=VS.85).aspx)

⁴⁹ For more information see [http://msdn.microsoft.com/en-us/library/ms724284\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ms724284(VS.85).aspx)

				The GetFileTime function ⁵⁰ can retrieve the last accessed time.
c_time	oval-sc:EntityItemIntType	0..1	false	<p>The date and time that the file was created.</p> <p>This is valid on NTFS formatted disk drives, but, not on FAT formatted disk drives.</p> <p>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.</p> <p>The GetFileTime function⁵² can retrieve the creation time.</p>
m_time	oval-sc:EntityItemIntType	0..1	false	<p>The date and time that the file was last modified.</p> <p>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.</p>

⁵⁰ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms724320\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms724320(v=vs.85).aspx)

⁵¹ For more information see [http://msdn.microsoft.com/en-us/library/ms724284\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ms724284(VS.85).aspx)

⁵² For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms724320\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms724320(v=vs.85).aspx)

⁵³ For more information see [http://msdn.microsoft.com/en-us/library/ms724284\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ms724284(VS.85).aspx)

				The GetFileTime function 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 .
version	oval-sc: EntityItemVersionType	0..1	false	The version number of the file. This value can be obtained via the VarQueryValue function ⁵⁶ or the FileVersionInfo class ⁵⁷ .
type	win-sc: EntityItemFileTypeType	0..1	false	The type of the file. This value can be obtained using the GetFileType function ⁵⁸ with the exception of FILE_ATTRIBUTE_DIRECTORY which is obtained by looking at the GetFileAttributesEx function 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

⁵⁴ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms724320\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms724320(v=vs.85).aspx)

⁵⁵ For more information see [http://msdn.microsoft.com/en-us/library/ms680355\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ms680355(VS.85).aspx)

⁵⁶ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464(v=vs.85).aspx)

⁵⁷ For more information see <http://msdn.microsoft.com/en-us/library/system.diagnostics.fileversioninfo.aspx>

⁵⁸ For more information see [http://msdn.microsoft.com/en-us/library/aa364960\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa364960(VS.85).aspx)

⁵⁹ For more information see [http://msdn.microsoft.com/en-us/library/aa364946\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa364946(VS.85).aspx)

				<p>releases (GDR) development environment and the quick fix engineering (QFE) development environment.</p> <p>This value MUST be the text prior to the mmmmmm-nnnn component of the file version formats⁶⁰.</p> <p>This value can be obtained via the VarQueryValue function⁶¹.</p>
company	oval-sc: EntityItemStringType	0..1	false	<p>The name of the company that created the file.</p> <p>This value can be obtained via the VarQueryValue function⁶² or the FileVersionInfo class⁶³.</p>
internal_name	oval-sc: EntityItemStringType	0..1	false	<p>The internal name of the file.</p> <p>This value can be obtained via the VarQueryValue function⁶⁴ or the FileVersionInfo class⁶⁵.</p>
language	oval-sc: EntityItemStringType	0..1	false	<p>The description string for the Microsoft Language Identifier associated with the file.</p>

⁶⁰ For more information see <http://support.microsoft.com/kb/824994>

⁶¹ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464(v=vs.85).aspx)

⁶² For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464(v=vs.85).aspx)

⁶³ For more information see <http://msdn.microsoft.com/en-us/library/system.diagnostics.fileversioninfo.aspx>

⁶⁴ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464(v=vs.85).aspx)

⁶⁵ For more information see <http://msdn.microsoft.com/en-us/library/system.diagnostics.fileversioninfo.aspx>

				This value can be obtained via the VarQueryValue function ⁶⁶ or the FileVersionInfo class 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 or the FileVersionInfo class 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 or the FileVersionInfo class 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 or the FileVersionInfo class ⁷³ .
windows_view	win-sc: EntityItemWindowsViewType	0..1	false	The targeted file system view ⁷⁴ where the file or directory was

⁶⁶ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464(v=vs.85).aspx)

⁶⁷ For more information see <http://msdn.microsoft.com/en-us/library/system.diagnostics.fileversioninfo.aspx>

⁶⁸ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464(v=vs.85).aspx)

⁶⁹ For more information see <http://msdn.microsoft.com/en-us/library/system.diagnostics.fileversioninfo.aspx>

⁷⁰ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464(v=vs.85).aspx)

⁷¹ For more information see <http://msdn.microsoft.com/en-us/library/system.diagnostics.fileversioninfo.aspx>

⁷² For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms647464(v=vs.85).aspx)

⁷³ For more information see <http://msdn.microsoft.com/en-us/library/system.diagnostics.fileversioninfo.aspx>

⁷⁴ For more information see [http://msdn.microsoft.com/en-us/library/aa384187\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/aa384187(v=vs.85).aspx)

				collected.
--	--	--	--	------------

2.7 win-def:EntityStateFileTypeType

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

Enumeration Value	Description
<code>FILE_ATTRIBUTE_DIRECTORY</code>	This value indicates a directory.
<code>FILE_TYPE_CHAR</code>	This value indicates a character file, typically an LPT device or a console.
<code>FILE_TYPE_DISK</code>	This value indicates a disk file.
<code>FILE_TYPE_PIPE</code>	This value indicates a socket, a named pipe, or an anonymous pipe.
<code>FILE_TYPE_REMOTE</code>	This value is currently unused by Microsoft.
<code>FILE_TYPE_UNKNOWN</code>	This value indicates that the type of file is unknown.
<code><empty string></code>	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.

2.8 win-sc:EntityItemFileTypeType

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

Enumeration Value	Description
<code>FILE_ATTRIBUTE_DIRECTORY</code>	This value indicates a directory.
<code>FILE_TYPE_CHAR</code>	This value indicates a character file, typically an LPT device or a console.
<code>FILE_TYPE_DISK</code>	This value indicates a disk file.
<code>FILE_TYPE_PIPE</code>	This value indicates a socket, a named pipe, or an anonymous pipe.
<code>FILE_TYPE_REMOTE</code>	This value is currently unused by Microsoft.
<code>FILE_TYPE_UNKNOWN</code>	This value indicates that the type of file is unknown.
<code><empty string></code>	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.

2.12. win-def:EntityStateWindowsViewType

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

Enumeration Value	Description
<code>32_bit</code>	This value indicates the 32-bit view.
<code>64_bit</code>	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.
-----------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------

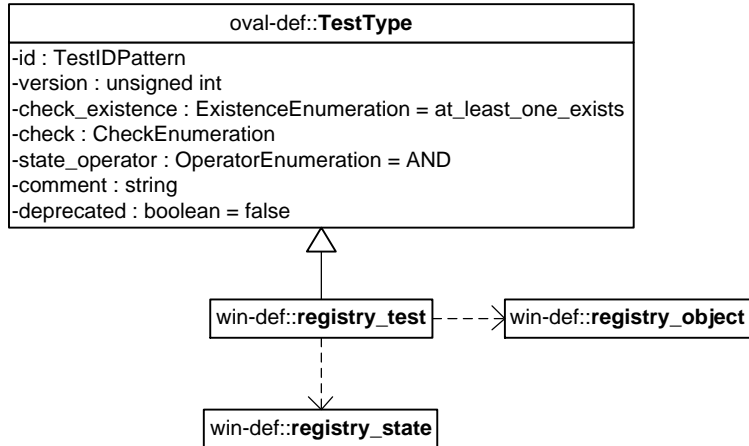
2.13. win-sc:EntityItemWindowsViewType

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.

2.14. win-def:registry_test

The `registry_test` is used to make assertions about information associated with the hives and keys in the registry⁷⁵ on Microsoft Windows operating systems. The `registry_test` MUST reference one `registry_object` and zero or more `registry_states`.



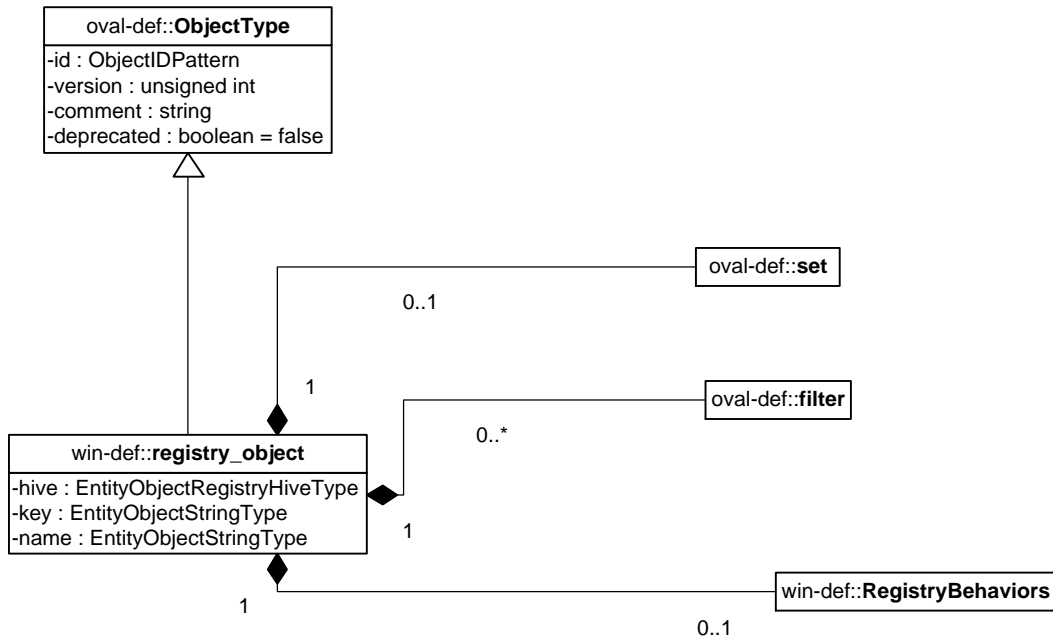
2.14.1. Known Supported Platforms

- Windows XP
- Windows Vista
- Windows 7

2.15. 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`.

⁷⁵ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms724182\(v=VS.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms724182(v=VS.85).aspx)



Property	Type	Multiplicity	Nullable	Description
set	oval-def:set	0..1	false	<p>Enables the expression of complex <code>registry_objects</code> that are the result of logically combining and filtering the <code>registry_items</code> that are identified by one or more <code>registry_objects</code>.</p> <p>The behaviors, hive, key, name, and filter properties MUST NOT be specified when this property is specified.</p> <p>Please see the OVAL Language Specification [2] for additional information.</p>
behaviors	win-def:RegistryBehaviors	0..1	false	<p>Specifies the behaviors that direct how the <code>registry_object</code> collects <code>registry_items</code> from the system.</p>
hive	win-def:EntityObjectRegistryHiveType	0..1	false	<p>The hive that the registry key belongs to.</p> <p>This SHOULD align with the</p>

				guidance provided in the MSDN documentation ⁷⁶ .
key	oval-def: EntityObjectStringType	1..1	true	<p>The registry key to be collected.</p> <p>This property MUST NOT include the hive as it must be specified in the hive property.</p> <p>xsi:nil="true" indicates that the <code>registry_object</code> must collect the set of hives specified by the hive entity. In this case, a value MUST NOT be specified.</p>
name	oval-def: EntityObjectStringType	1..1	true	<p>The name assigned to a value associated with a specific registry key.</p> <p>If an empty string is specified, the registry key's default value MUST be collected.</p> <p>xsi:nil="true" indicates that the <code>registry_object</code> must collect the <code>registry_items</code> specified by the hive and key properties. In this case, a value MUST NOT be specified.</p>
filter	oval-def:filter [2]	0..*	false	<p>Allows for the explicit inclusion or exclusion of <code>registry_items</code> from the set of <code>registry_items</code> collected by a <code>registry_object</code>.</p> <p>Please see the OVAL Language Specification [2] for additional information.</p>

⁷⁶ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms724836\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms724836(v=vs.85).aspx)

2.16. 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.

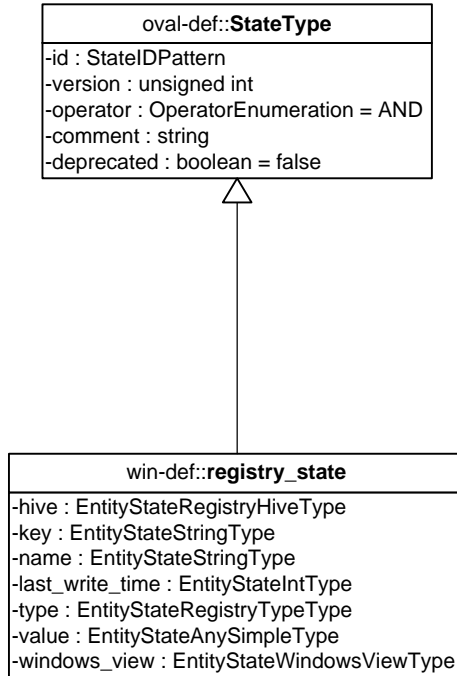
Attribute	Type	Possible Values	Description
max_depth	integer	< -1 -1 0 > 0	<p>Defines the maximum depth of registry traversal when the recurse_direction behavior is set to a value other than 'none'.</p> <p>< -1: not permitted.</p> <p>-1: traverse the registry with no limitation.</p> <p>0: do not traverse the registry.</p> <p>> 0: traverse the registry for the specified number of levels.</p> <p>Default Value: -1</p>
recurse_direction	string	'none' 'up' 'down'	<p>Defines the direction to recursively visit the registry.</p> <p>'none': do not traverse the registry.</p> <p>'up': traverse the registry by recursively visiting the parent keys.</p>

			<p><i>'down'</i>: traverse the registry by recursively visiting the child keys.</p> <p>Note: It is not an error if <code>max_depth</code> specifies a certain level of traversal and that level does not exist.</p> <p>Default Value: none</p>
windows_view	string	<p><i>'32_bit'</i></p> <p><i>'64_bit'</i></p>	<p>64-bit versions of Windows provide an alternate registry view to 32-bit applications⁷⁷. This behavior defines which view should be examined by the <code>registry_object</code>.</p> <p><i>'32_bit'</i>: check the 32_bit view of the registry.</p> <p><i>'64_bit'</i>: check the 64_bit view of the registry.</p> <p>This behavior only applies to 64-bit versions of Windows and MUST NOT be applied on other platforms.</p> <p>Default Value: 64-bit</p>

⁷⁷ For more information see [http://msdn.microsoft.com/en-us/library/aa384187\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/aa384187(v=vs.85).aspx)

2.17. 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	Nilable	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 .
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.

⁷⁸For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms724836\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms724836(v=vs.85).aspx)

				<p>If an empty string is specified, the registry key's default value MUST be collected.</p> <p>This can be obtained using the RegQueryValueEx function⁷⁹.</p>
last_write_time	oval-def:EntityStateIntType	0..1	false	<p>The date and time that the key or any of its value entries were modified.</p> <p>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.</p> <p>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</p>

⁷⁹ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms724911\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms724911(v=vs.85).aspx)

⁸⁰ For more information see [http://msdn.microsoft.com/en-us/library/ms724284\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ms724284(VS.85).aspx)

				<p>modified.</p> <p>Thus when collecting information about a registry name, the last write time does not correlate directly to the specified name.</p> <p>This can be obtained using the RegQueryInfoKey function⁸¹.</p>
type	win-def: EntityStateRegistryTypeType	0..1	false	<p>The type associated with the value of a hive or registry key.</p> <p>This can be obtained using the RegQueryValueEx function⁸².</p>
value	oval-def: EntityStateAnySimpleType	0..*	false	<p>The value(s) associated with a hive or registry key.</p> <p>The value of a hive or registry key can be obtained using the RegQueryValueEx function⁸³.</p> <p>Please see the OVAL Language Specification [2] for more information about how datatypes are assigned to OVAL Item Entities.</p>
windows_view	win-def: EntityStateWindowsViewType	0..1	false	<p>The targeted registry view⁸⁴ where the hive</p>

⁸¹ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms724902\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms724902(v=vs.85).aspx)

⁸² For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms724911\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms724911(v=vs.85).aspx)

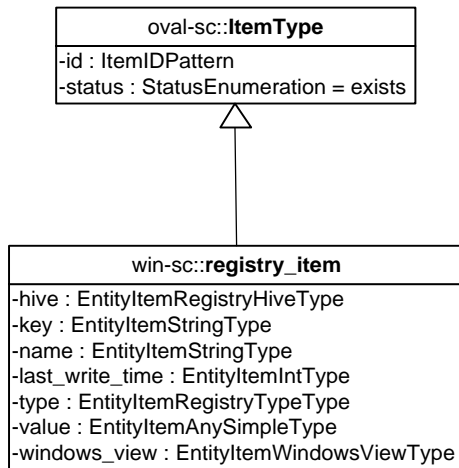
⁸³ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms724911\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms724911(v=vs.85).aspx)

⁸⁴ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms724072\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms724072(v=vs.85).aspx)

				or registry key was collected.
--	--	--	--	--------------------------------

2.18. 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	Nilable	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 .
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

⁸⁵For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms724836\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms724836(v=vs.85).aspx)

				<p>specified, the registry key's default value MUST be collected.</p> <p>This can be obtained using the RegQueryValueEx function⁸⁶.</p>
last_write_time	oval-sc:EntityItemIntType	0..1	false	<p>The date and time that the key or any of its value entries were last modified.</p> <p>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.</p> <p>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</p>

⁸⁶ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms724911\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms724911(v=vs.85).aspx)

⁸⁷ For more information see [http://msdn.microsoft.com/en-us/library/ms724284\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ms724284(VS.85).aspx)

				<p>registry name, the last write time does not correlate directly to the specified name.</p> <p>This can be obtained using the RegQueryInfoKey function⁸⁸.</p>
type	win-sc: EntityItemRegistryTypeType	0..1	false	<p>The type associated with the value of a hive or registry key.</p> <p>This can be obtained using the RegQueryValueEx function⁸⁹.</p>
value	oval-sc: EntityItemAnySimpleType	0..*	false	<p>The value(s) associated with a hive or registry key.</p> <p>The value of a hive or registry key can be obtained using the RegQueryValueEx function⁹⁰.</p> <p>Please see the OVAL Language Specification [2] for more information about how datatypes are assigned to OVAL Item Entities.</p>
windows_view	win-sc: EntityItemWindowsViewType	0..1	false	<p>The targeted registry view⁹¹ where the hive or registry key was collected.</p>

⁸⁸ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms724902\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms724902(v=vs.85).aspx)

⁸⁹ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms724911\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms724911(v=vs.85).aspx)

⁹⁰ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms724911\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms724911(v=vs.85).aspx)

⁹¹ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms724072\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms724072(v=vs.85).aspx)

2.19. win-def:EntityObjectRegistryHiveType

The `EntityObjectRegistryHiveType` defines the enumeration of possible hive types for the registry supported on Microsoft Windows platforms⁹².

Enumeration Value	Description
<code>HKEY_CLASSES_ROOT</code>	This value indicates file types with programs and configuration data for automation (e.g. COM objects and Visual Basic Programs).
<code>HKEY_CURRENT_CONFIG</code>	This value indicates configuration data for the current hardware profile.
<code>HKEY_CURRENT_USER</code>	This value indicates the user profile of the user that is currently logged into the system.
<code>HKEY_LOCAL_MACHINE</code>	This value indicates information about the local system.
<code>HKEY_USERS</code>	This value indicates user-specific data.
<code><empty string></code>	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.

2.20. win-def:EntityStateRegistryHiveType

The `EntityStateRegistryHiveType` defines the enumeration of possible hive types for the registry supported on Microsoft Windows platforms⁹³.

Enumeration Value	Description
<code>HKEY_CLASSES_ROOT</code>	This value indicates file types with programs and configuration data for automation (e.g. COM objects and Visual Basic Programs).
<code>HKEY_CURRENT_CONFIG</code>	This value indicates configuration data for the current hardware profile.
<code>HKEY_CURRENT_USER</code>	This value indicates the user profile of the user that is currently logged into the system.
<code>HKEY_LOCAL_MACHINE</code>	This value indicates information about the local system.
<code>HKEY_USERS</code>	This value indicates user-specific data.
<code><empty string></code>	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.

2.21. win-sc:EntityItemRegistryHiveType

The `EntityItemRegistryHiveType` defines the enumeration of possible hive types for the registry supported on Microsoft Windows platforms⁹⁴.

Enumeration Value	Description
<code>HKEY_CLASSES_ROOT</code>	This value indicates file types with programs and configuration data for automation (e.g. COM objects and Visual Basic Programs).
<code>HKEY_CURRENT_CONFIG</code>	This value indicates configuration data for the current hardware profile.
<code>HKEY_CURRENT_USER</code>	This value indicates the user profile of the user that is currently logged into the system.

⁹² For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms724836\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms724836(v=vs.85).aspx)

⁹³ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms724836\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms724836(v=vs.85).aspx)

⁹⁴ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms724836\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms724836(v=vs.85).aspx)

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.

2.22. win-def:EntityStateRegistryTypeType

The `EntityStateRegistryTypeType` defines the types⁹⁵ 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_dword_little_endian	The <code>reg_dword_little_endian</code> type is used by registry keys that specify a 32-bit little-endian number. It is designed to run on little-endian computer architectures.
reg_dword_big_endian	The <code>reg_dword_big_endian</code> type is used by registry keys that specify a 32-bit big-endian number. It is designed to run on big-endian computer architectures.
reg_expand_sz	This value indicates a null-terminated string that contains unexpanded references to environment variables.
reg_link	The <code>reg_link</code> type is used by the registry keys for null-terminated unicode strings. It is related to target path of a symbolic link created by the <code>RegCreateKeyEx</code> function.
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_qword_little_endian	The <code>reg_qword_little_endian</code> type is used by registry keys that specify a 64-bit little-endian number. It is designed to run on little-endian computer architectures.
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.

2.23. win-sc:EntityItemRegistryTypeType

The `EntityItemRegistryTypeType` defines the types⁹⁶ associated with the values of hives and registry keys in the registry on Microsoft Windows platforms.

⁹⁵ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms724884\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms724884(v=vs.85).aspx)

⁹⁶ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms724884\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms724884(v=vs.85).aspx)

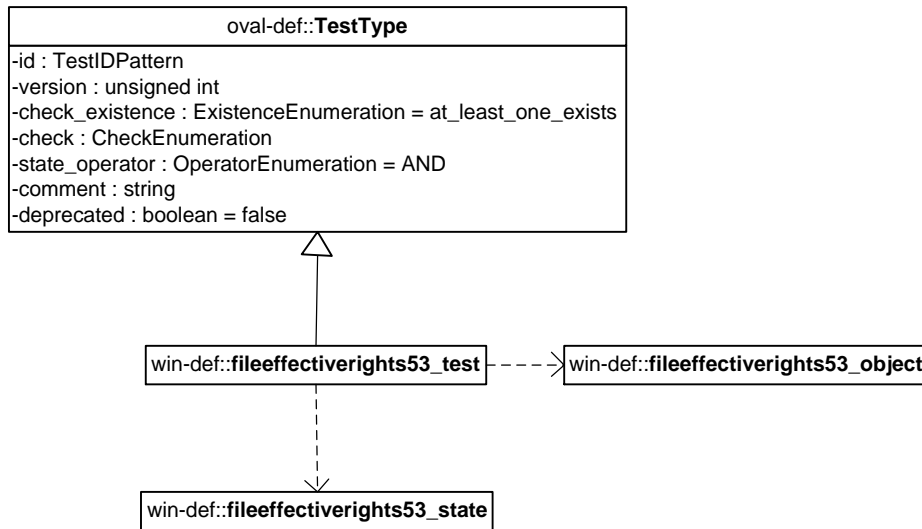
Enumeration Value	Description
reg_binary	This value indicates binary data in any form.
reg_dword	This value indicates a 32-bit number.
reg_dword_little_endian	The reg_dword_little_endian type is used by registry keys that specify a 32-bit little-endian number. It is designed to run on little-endian computer architectures.
reg_dword_big_endian	The reg_dword_big_endian type is used by registry keys that specify a 32-bit big-endian number. It is designed to run on big-endian computer architectures.
reg_expand_sz	This value indicates a null-terminated string that contains unexpanded references to environment variables.
reg_link	The reg_link type is used by the registry keys for null-terminated unicode strings. It is related to target path of a symbolic link created by the RegCreateKeyEx function.
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_qword_little_endian	The reg_qword_little_endian type is used by registry keys that specify a 64-bit little-endian number. It is designed to run on little-endian computer architectures.
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.

2.24. win-def:fileeffectiverights53_test

The fileeffectiverights53_test is used to make assertions about the effective rights of files on Microsoft Windows operating systems⁹⁷. The fileeffectiverights53_test MUST reference one fileeffectiverights53_object and zero or more

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/aa364399(v=vs.85).aspx) , [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607\(v=vs.85\).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>

fileeffectiverights53_states.



2.24.1. Known Supported Platforms

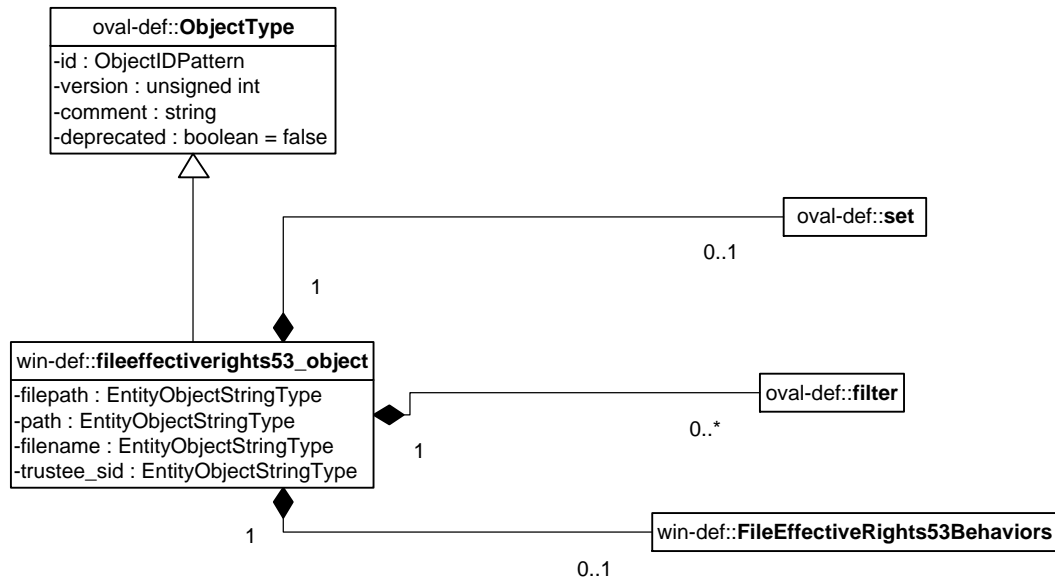
- Windows XP
- Windows Vista
- Windows 7

2.25. win-def:fileeffectiverights53_object

The `fileeffectiverights53_object` construct defines the set of files and directories and the trustee SID(s)⁹⁸ whose associated effective rights information should be collected and represented as `fileeffectiverights53_items`. The `fileeffectiverights53_object` is capable of collecting

⁹⁸ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379571\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379571(v=vs.85).aspx)

directories and all file types as defined in the EntityStateFileTypeType



Property	Type	Multiplicity	Nullable	Description
Set	oval-def:set	0..1	false	<p>Enables the expression of complex fileeffectiverights 53_objects that are the result of logically combining and filtering the fileeffectiverights 53_items that are identified by one or more fileeffectiverights 53_objects.</p> <p>The behaviors, filepath, path, filename, trustee_sid, and filter properties MUST NOT be specified when this property is specified.</p> <p>Please see the OVAL Language Specification [2] for additional information.</p>
behaviors	win-def:FileEffectiveRights53Behaviors	0..1	false	<p>Specifies the behaviors that direct how the fileeffectiverights 53_object collects fileeffectiverights 53_items from the</p>

				system.
filepath	oval-def: EntityObjectStringType	0..1	false	<p>The absolute path to a file on the system.</p> <p>The absolute path SHOULD align with the guidance provided in the MSDN documentation⁹⁹.</p> <p>A directory MUST NOT be specified for this property.</p> <p>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.</p>
path	oval-def: EntityObjectStringType	0..1	false	<p>The directory component of the absolute path to a directory or file on the system.</p> <p>The path component SHOULD align with the guidance provided in the MSDN documentation¹⁰⁰.</p> <p>The filepath property MUST NOT be specified when this property is specified.</p>
filename	oval-def: EntityObjectStringType	0..1	true	<p>The name of a file to evaluate.</p> <p>A filename MUST NOT contain the characters in the set {/, \, ?, , >, :, *}. The filename SHOULD also align with the guidance provided in the MSDN</p>

⁹⁹ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa365247\(v=vs.85\).aspx#paths](http://msdn.microsoft.com/en-us/library/windows/desktop/aa365247(v=vs.85).aspx#paths)

¹⁰⁰ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa365247\(v=vs.85\).aspx#paths](http://msdn.microsoft.com/en-us/library/windows/desktop/aa365247(v=vs.85).aspx#paths)

				<p>documentation, as there are more conventions when naming files beyond the characters listed above¹⁰¹.</p> <p>xsi:nil="true" indicates that the <code>fileeffectiverights53_object</code> MUST collect the set of directories specified by the path entity. In addition, a value for the filename entity MUST NOT be specified.</p>
trustee_sid	oval-def: EntityObjectStringType	1..1	false	<p>The unique security identifier associated with a user account, group account, or logon session.</p> <p>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 descriptor¹⁰².</p>
filter	oval-def:filter	0..*	false	<p>Allows for the explicit inclusion or exclusion of <code>fileeffectiverights53_items</code> from the set of <code>fileeffectiverights53_items</code> collected by a <code>fileeffectiverights53_object</code>.</p> <p>Please see the OVAL Language Specification [2] for additional information.</p>

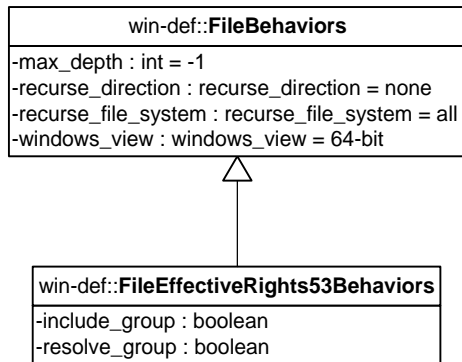
2.26. FileEffectiveRights53Behaviors

The FileEffectiveRights53Behaviors construct defines the behaviors that direct how the `fileeffectiverights53_object` collects `fileeffectiverights53_items` from the

¹⁰¹ For more information see <http://msdn.microsoft.com/en-us/library/aa365247.aspx>

¹⁰² For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379166\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379166(v=vs.85).aspx)

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.



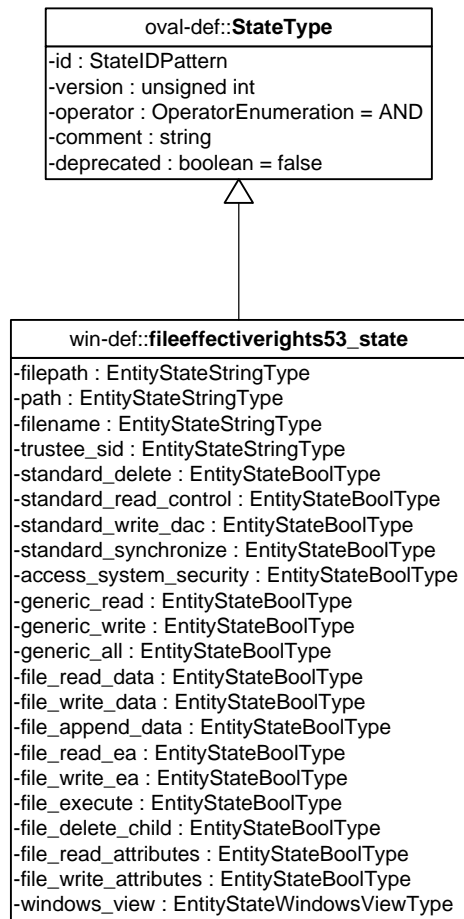
Attribute	Type	Possible Values	Description
include_group	boolean	'true' 'false'	<p>Defines whether or not the group SID should be collected when the trustee_sid property specifies a group SID.</p> <p>'true': The group SID MUST be collected when the trustee_sid property specifies a group SID.</p> <p>'false': The group SID MUST NOT be collected when the trustee_sid property specifies a group SID.</p> <p>Default Value: true</p>
resolve_group	boolean	'true' 'false'	<p>Defines whether or not the members of group SIDs should be resolved and collected.</p> <p>Note that all child</p>

			<p>groups should also be resolved and any valid domain accounts that are members should also be included.</p> <p>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.</p> <p>'true': The members of a group SID <u>MUST</u> be resolved and collected.</p> <p>'false': The members of a group SID <u>MUST NOT</u> be resolved or collected.</p> <p>Default Value: false</p>
--	--	--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

2.27. 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 permissions¹⁰³.

¹⁰³ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa446645\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa446645(v=vs.85).aspx)



Property	Type	Multiplicity	Nilable	Description
filepath	oval-def: EntityStateStringType	0..1	false	<p>The absolute path to a file on the system.</p> <p>The absolute path SHOULD align with the guidance provided in the MSDN documentation¹⁰⁴.</p> <p>A directory MUST NOT be specified for this property.</p> <p>The max_depth and recurse_direction</p>

¹⁰⁴ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa365247\(v=vs.85\).aspx#paths](http://msdn.microsoft.com/en-us/library/windows/desktop/aa365247(v=vs.85).aspx#paths)

				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	<p>The directory component of the absolute path to a directory or file on the system.</p> <p>The path component SHOULD align with the guidance provided in the MSDN documentation¹⁰⁵.</p> <p>The filepath property MUST NOT be specified when this property is specified.</p>
filename	oval-def: EntityStateStringType	0..1	false	<p>The name of a file to evaluate.</p> <p>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 above¹⁰⁶.</p>

¹⁰⁵ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa365247\(v=vs.85\).aspx#paths](http://msdn.microsoft.com/en-us/library/windows/desktop/aa365247(v=vs.85).aspx#paths)

¹⁰⁶ For more information see <http://msdn.microsoft.com/en-us/library/aa365247.aspx>

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 .
standard_delete	oval-def: EntityStateBoolType	0..1	false	The right to delete the file 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 .
standard_write_dac	oval-def: EntityStateBoolType	0..1	false	The right to modify the DACL in the file's Security Descriptor ¹¹⁰ .
standard_write_owner	oval-def: EntityStateBoolType	0..1	false	The right to change the owner in the file's Security Descriptor ¹¹¹ .
standard_synchronize	oval-def: EntityStateBoolType	0..1	false	The right to use the file for synchronization. This enables a thread to

¹⁰⁷ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379166\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379166(v=vs.85).aspx)

¹⁰⁸ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx)

¹⁰⁹ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx)

¹¹⁰ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx)

¹¹¹ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx)

				wait until the file is in the signaled state ¹¹² .
access_system_security	oval-def: EntityStateBoolType	0..1	false	Indicates access to a system access control list (SACL) ¹¹³ .
generic_read	oval-def: EntityStateBoolType	0..1	false	Read access ¹¹⁴ .
generic_write	oval-def: EntityStateBoolType	0..1	false	Write access ¹¹⁵ .
generic_execute	oval-def: EntityStateBoolType	0..1	false	Execute access ¹¹⁶ .
generic_all	oval-def: EntityStateBoolType	0..1	false	Read, write, and execute access 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 .
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 .
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 .
file_read_ea	oval-def: EntityStateBoolType	0..1	false	Grants the right to read extended attribute ¹²¹ .
file_write_ea	oval-def:	0..1	false	Grants the right to

¹¹² For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx)

¹¹³ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx)

¹¹⁴ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632\(v=VS.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632(v=VS.85).aspx)

¹¹⁵ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632\(v=VS.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632(v=VS.85).aspx)

¹¹⁶ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632\(v=VS.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632(v=VS.85).aspx)

¹¹⁷ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632\(v=VS.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632(v=VS.85).aspx)

¹¹⁸ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116(v=vs.85).aspx)

¹¹⁹ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116(v=vs.85).aspx)

¹²⁰ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116(v=vs.85).aspx)

¹²¹ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116(v=vs.85).aspx)

	EntityStateBoolType			write extended attributes 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 .
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 .
file_read_attributes	oval-def: EntityStateBoolType	0..1	false	Grants the right to read file, or directory, attributes ¹²⁵ .
file_write_attributes	oval-def: EntityStateBoolType	0..1	false	Grants the right to change file, or directory, attributes ¹²⁶ .
windows_view	win-def: EntityStateWindowsViewType	0..1	false	The targeted file system view ¹²⁷ where the file or directory was collected.

2.28. 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.

¹²² For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116(v=vs.85).aspx)

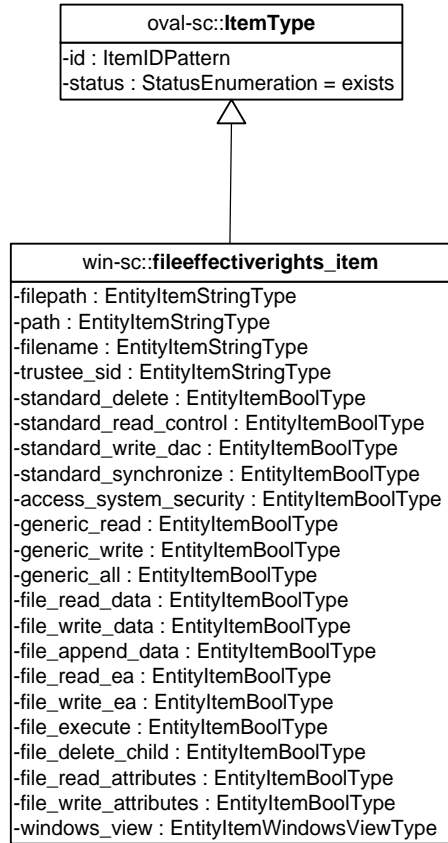
¹²³ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116(v=vs.85).aspx)

¹²⁴ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116(v=vs.85).aspx)

¹²⁵ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116(v=vs.85).aspx)

¹²⁶ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116(v=vs.85).aspx)

¹²⁷ For more information see [http://msdn.microsoft.com/en-us/library/aa384187\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/aa384187(v=vs.85).aspx)



Property	Type	Multiplicity	Nullable	Description
filepath	oval-sc: EntityItemStringType	0..1	false	<p>The absolute path to a file on the system.</p> <p>The absolute path SHOULD align with the guidance provided in the MSDN documentation¹²⁸.</p> <p>A directory MUST NOT be specified for this property.</p> <p>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</p>

¹²⁸ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa365247\(v=vs.85\).aspx#paths](http://msdn.microsoft.com/en-us/library/windows/desktop/aa365247(v=vs.85).aspx#paths)

				filename properties.
path	oval-sc: EntityItemStringType	0..1	false	<p>The directory component of the absolute path to a directory or file on the system.</p> <p>The path component SHOULD align with the guidance provided in the MSDN documentation¹²⁹.</p> <p>The filepath property MUST NOT be specified when this property is specified.</p>
filename	oval-sc: EntityItemStringType	0..1	true	<p>The name of a file to evaluate.</p> <p>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 above¹³⁰.</p>
trustee_sid	oval-sc: EntityItemStringType	0..1	false	<p>The unique security identifier associated with a user account, group account, or logon session.</p> <p>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 descriptor¹³¹.</p>

¹²⁹ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa365247\(v=vs.85\).aspx#paths](http://msdn.microsoft.com/en-us/library/windows/desktop/aa365247(v=vs.85).aspx#paths)

¹³⁰ For more information see <http://msdn.microsoft.com/en-us/library/aa365247.aspx>

¹³¹ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379166\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379166(v=vs.85).aspx)

standard_delete	oval-sc:EntityItemBoolType	0..1	false	The right to delete the file 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 .
standard_write_dac	oval-sc:EntityItemBoolType			The right to modify the DACL in the file's Security Descriptor ¹³⁴ .
standard_write_owner	oval-sc:EntityItemBoolType	0..1	false	The right to change the owner in the file's Security Descriptor 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 .
access_system_security	oval-sc:EntityItemBoolType	0..1	false	Indicates access to a system access control list (SACL) ¹³⁷ .
generic_read	oval-sc:EntityItemBoolType	0..1	false	Read access ¹³⁸ .
generic_write	oval-sc:EntityItemBoolType	0..1	false	Write access ¹³⁹ .
generic_execute	oval-sc:EntityItemBoolType	0..1	false	Execute access ¹⁴⁰ .
generic_all	oval-sc:EntityItemBoolType	0..1	false	Read, write, and execute access 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 .
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 .
file_append_data	oval-sc:EntityItemBoolType	0..1	false	Grants the right to append

¹³² For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx)

¹³³ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx)

¹³⁴ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx)

¹³⁵ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx)

¹³⁶ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx)

¹³⁷ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx)

¹³⁸ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632\(v=VS.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632(v=VS.85).aspx)

¹³⁹ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632\(v=VS.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632(v=VS.85).aspx)

¹⁴⁰ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632\(v=VS.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632(v=VS.85).aspx)

¹⁴¹ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632\(v=VS.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632(v=VS.85).aspx)

¹⁴² For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116(v=vs.85).aspx)

¹⁴³ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116(v=vs.85).aspx)

				data to the file, or if a directory, grants the right to add a sub-directory to the directory ¹⁴⁴ .
file_read_ea	oval-sc:EntityItemBoolType	0..1	false	Grants the right to read extended attribute ¹⁴⁵ .
file_write_ea	oval-sc:EntityItemBoolType	0..1	false	Grants the right to write extended attributes 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 .
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 .
file_read_attributes	oval-sc:EntityItemBoolType	0..1	false	Grants the right to read file, or directory, attributes ¹⁴⁹ .
file_write_attributes	oval-sc:EntityItemBoolType	0..1	false	Grants the right to change file, or directory, attributes ¹⁵⁰ .
windows_view	win-sc:EntityItemWindowsViewType	0..1	false	The targeted file system view ¹⁵¹ where the file or directory was collected.

¹⁴⁴ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116(v=vs.85).aspx)

¹⁴⁵ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116(v=vs.85).aspx)

¹⁴⁶ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116(v=vs.85).aspx)

¹⁴⁷ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116(v=vs.85).aspx)

¹⁴⁸ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116(v=vs.85).aspx)

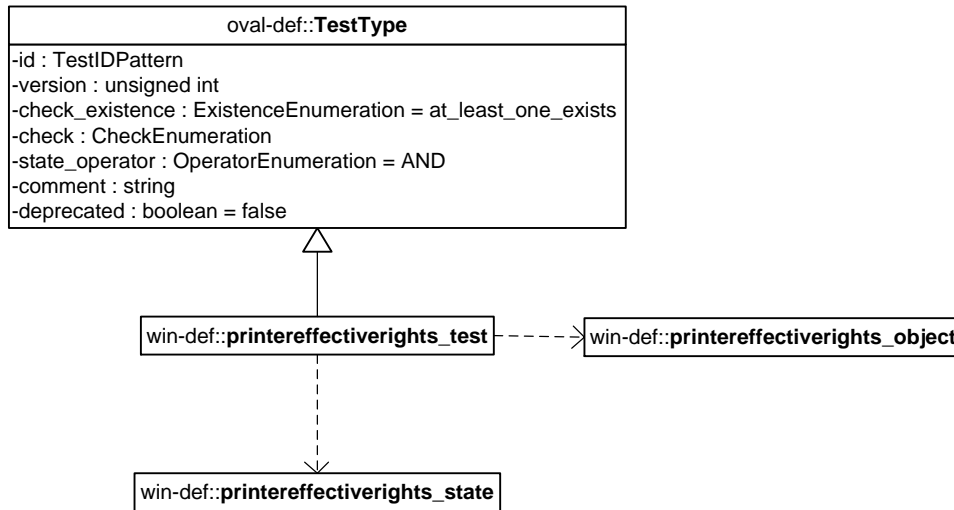
¹⁴⁹ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116(v=vs.85).aspx)

¹⁵⁰ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116(v=vs.85).aspx)

¹⁵¹ For more information see [http://msdn.microsoft.com/en-us/library/aa384187\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/aa384187(v=vs.85).aspx)

2.29. win-def:printereffectiverights_test

The `printereffectiverights_test` is used to make assertions about the effective rights of Windows printers¹⁵². The `printereffectiverights53_test` MUST reference one `printereffectiverights53_object` and zero or more `printereffectiverights53_states`.



2.29.1. Known Supported Platforms

- Windows XP
- Windows Vista
- Windows 7

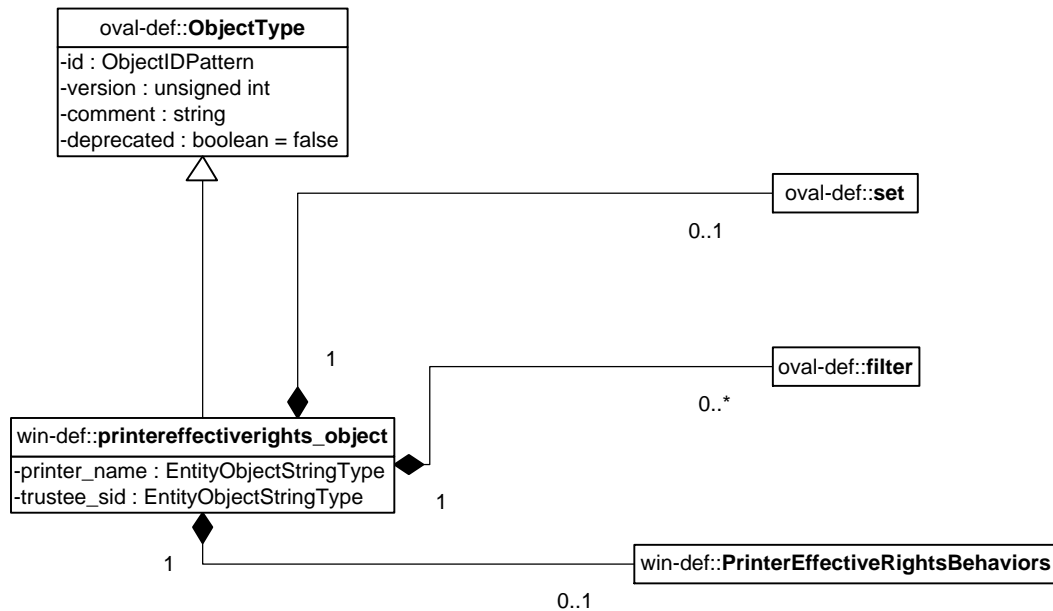
2.30. win-def:printereffectiverights_object

The `printereffectiverights_object` construct defines the set of printers and SIDs¹⁵³ 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

¹⁵² For more information see [http://msdn.microsoft.com/en-us/library/cc244650\(v=PROT.10\).aspx](http://msdn.microsoft.com/en-us/library/cc244650(v=PROT.10).aspx)

¹⁵³ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379571\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379571(v=vs.85).aspx)

effective rights object.



Property	Type	Multiplicity	Nullable	Description
set	oval-def:set	0..1	false	Enables the expression of complex <code>printereffectiverights_objects</code> that are the result of logically combining and filtering the <code>printereffectiverights_items</code> that are identified by one or more <code>printereffectiverights_objects</code> .
behaviors	win-def:PrinterEffectiveRightsBehaviors	0..1	false	Specifies the behaviors that direct how the <code>printereffectiverights_object</code> collects <code>printereffectiverights_items</code> 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:	0..1	true	The unique SID associated

	EntityObjectStringType			<p>with a user, group, system, or program (such as a Windows service).</p> <p>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 Descriptor¹⁵⁴.</p>
filter	oval-def:filter [2]	0..*	false	<p>Allows for the explicit inclusion or exclusion of <code>printereffectiverights_items</code> from the set of <code>printereffectiverights_items</code> collected by a <code>printereffectiverights_object</code>.</p> <p>Please see the OVAL Language Specification [2] for additional information.</p>

2.31. 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.

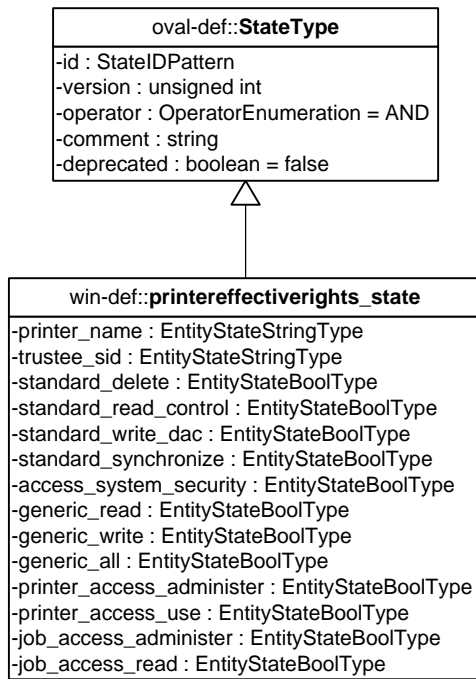
Attribute	Type	Possible Values	Description
include_group	bool	'true' 'false'	Defines whether or not the group SID should be collected when the <code>trustee_sid</code> property specifies a group SID.

¹⁵⁴ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379166\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379166(v=vs.85).aspx)

			<p><i>'true'</i>: The group SID <u>MUST</u> be collected when the trustee_sid property specifies a group SID.</p> <p><i>'false'</i>: The group SID <u>MUST NOT</u> be collected when the trustee_sid property specifies a group SID.</p> <p>Default Value: true</p>
resolve_group	bool	<p><i>'true'</i></p> <p><i>'false'</i></p>	<p>Defines whether or not the members of group SIDs should be resolved and collected.</p> <p>Note that all child groups should also be resolved and any valid domain accounts that are members should also be included.</p> <p>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.</p> <p><i>'true'</i>: The members of a group SID <u>MUST</u> be resolved and collected.</p> <p><i>'false'</i>: The members of a group SID <u>MUST NOT</u> be resolved or collected.</p> <p>Default Value: false</p>

2.32. 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	Nullable	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 .
standard_delete	oval-def: EntityStateBoolType	0..1	false	The right to delete the printer object ¹⁵⁶ .
standard_read_cont	oval-def:	0..1	false	The right to read the

¹⁵⁵ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379166\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379166(v=vs.85).aspx)

¹⁵⁶ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx)

rol	EntityStateBoolType			information in the printer object's Security Descriptor, not including the information in the system access control list (SACL) ¹⁵⁷ .
standard_write_dac	oval-def: EntityStateBoolType	0..1	false	The right to modify the DACL in the printer object's Security Descriptor ¹⁵⁸ .
standard_write_owner	oval-def: EntityStateBoolType	0..1	false	The right to change the owner in the printer object's Security Descriptor 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 .
access_system_security	oval-def: EntityStateBoolType	0..1	false	Indicates access to a system access control list (SACL) ¹⁶¹ .
generic_read	oval-def: EntityStateBoolType	0..1	false	Read access ¹⁶² .
generic_write	oval-def: EntityStateBoolType	0..1	false	Write access ¹⁶³ .
generic_execute	oval-def: EntityStateBoolType	0..1	false	Execute access ¹⁶⁴ .
generic_all	oval-def: EntityStateBoolType	0..1	false	Read, write, and execute access ¹⁶⁵ .
printer_access_administer	oval-def: EntityStateBoolType	0..1	false	Access to perform administrative tasks ¹⁶⁶ , which include pausing the printer, deleting all print jobs, resuming a paused printer, and setting the printer status ¹⁶⁷ .

¹⁵⁷ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx)

¹⁵⁸ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx)

¹⁵⁹ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx)

¹⁶⁰ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx)

¹⁶¹ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx)

¹⁶² For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632\(v=VS.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632(v=VS.85).aspx)

¹⁶³ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632\(v=VS.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632(v=VS.85).aspx)

¹⁶⁴ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632\(v=VS.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632(v=VS.85).aspx)

¹⁶⁵ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632\(v=VS.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632(v=VS.85).aspx)

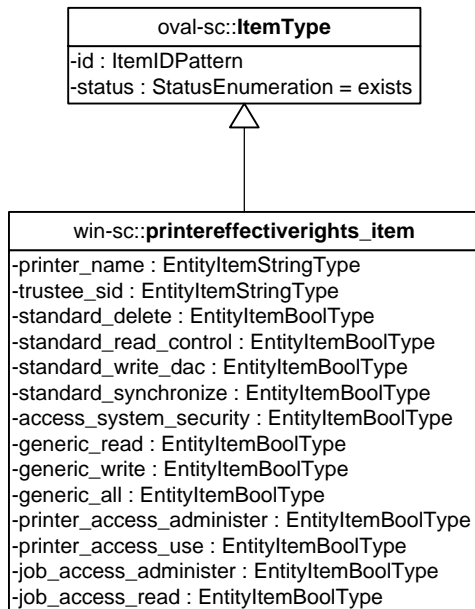
¹⁶⁶ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/dd162751\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/dd162751(v=vs.85).aspx)

¹⁶⁷ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/dd145082\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/dd145082(v=vs.85).aspx)

printer_access_use	oval-def: EntityStateBoolType	0..1	false	Access to perform basic printing operations ¹⁶⁸ .
job_access_adminis- ter	oval-def: EntityStateBoolType	0..1	false	Printer-specific authorization to cancel, pause, resume, or restart the job ¹⁶⁹ .
job_access_read	oval-def: EntityStateBoolType	0..1	false	Printing-specific read rights for the spool file ¹⁷⁰ .

2.33. 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	Multiplic- ity	Nilla- ble	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.

¹⁶⁸ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/dd162751\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/dd162751(v=vs.85).aspx)

¹⁶⁹ For more information see [http://msdn.microsoft.com/en-us/library/cc244650\(v=PROT.10\).aspx](http://msdn.microsoft.com/en-us/library/cc244650(v=PROT.10).aspx)

¹⁷⁰ For more information see [http://msdn.microsoft.com/en-us/library/cc244650\(v=PROT.10\).aspx](http://msdn.microsoft.com/en-us/library/cc244650(v=PROT.10).aspx)

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 .
standard_delete	oval-sc:EntityItemBoolType	0..1	false	The right to delete the printer object 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 .
standard_write_dac	oval-sc:EntityItemBoolType	0..1	false	The right to modify the DACL in the printer object's Security Descriptor ¹⁷⁴ .
standard_write_owner	oval-sc:EntityItemBoolType	0..1	false	The right to change the owner in the printer object's Security Descriptor 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 .
access_system_security	oval-sc:EntityItemBoolType	0..1	false	Indicates access to a system access control list (SACL) ¹⁷⁷ .
generic_read	oval-sc:EntityItemBoolType	0..1	false	Read access ¹⁷⁸ .
generic_write	oval-sc:EntityItemBoolType	0..1	false	Write access ¹⁷⁹ .
generic_execute	oval-sc:EntityItemBoolType	0..1	false	Execute access ¹⁸⁰ .
generic_all	oval-sc:EntityItemBoolType	0..1	false	Read, write, and execute access ¹⁸¹ .

¹⁷¹ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379166\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379166(v=vs.85).aspx)

¹⁷² For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx)

¹⁷³ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx)

¹⁷⁴ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx)

¹⁷⁵ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx)

¹⁷⁶ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx)

¹⁷⁷ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx)

¹⁷⁸ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632\(v=VS.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632(v=VS.85).aspx)

¹⁷⁹ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632\(v=VS.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632(v=VS.85).aspx)

¹⁸⁰ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632\(v=VS.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632(v=VS.85).aspx)

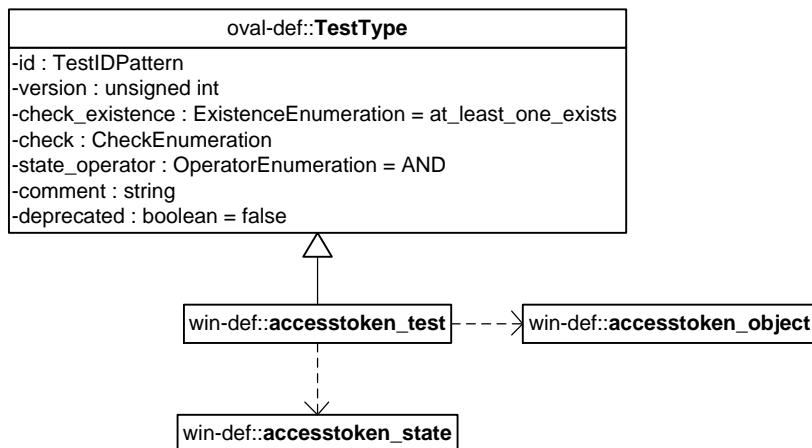
¹⁸¹ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632\(v=VS.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632(v=VS.85).aspx)

printer_access_administer	oval-sc:EntityItemBoolType	0..1	false	Access to perform administrative tasks ¹⁸² , which include pausing the printer, deleting all print jobs, resuming a paused printer, and setting the printer status ¹⁸³ .
printer_access_use	oval-sc:EntityItemBoolType	0..1	false	Access to perform basic printing operations ¹⁸⁴ .
job_access_administer	oval-sc:EntityItemBoolType	0..1	false	Printer-specific authorization to cancel, pause, resume, or restart the job ¹⁸⁵ .
job_access_read	oval-sc:EntityItemBoolType	0..1	false	Printing-specific read rights for the spool file ¹⁸⁶ .

2.34. win-def:acesstoken_test

The `acesstoken_test` is used to make assertions about the properties of Windows access tokens as well as individual privileges and rights associated with them¹⁸⁷. The `acesstoken_test` MUST reference one `acesstoken_object` and zero or more `acesstoken_states`.

This test has been deprecated and will be removed in version 6.0 of the language. Due to scalability issues, it is encouraged that you use the `userright_test`.



¹⁸² For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/dd162751\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/dd162751(v=vs.85).aspx)

¹⁸³ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/dd145082\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/dd145082(v=vs.85).aspx)

¹⁸⁴ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/dd162751\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/dd162751(v=vs.85).aspx)

¹⁸⁵ For more information see [http://msdn.microsoft.com/en-us/library/cc244650\(v=PROT.10\).aspx](http://msdn.microsoft.com/en-us/library/cc244650(v=PROT.10).aspx)

¹⁸⁶ For more information see [http://msdn.microsoft.com/en-us/library/cc244650\(v=PROT.10\).aspx](http://msdn.microsoft.com/en-us/library/cc244650(v=PROT.10).aspx)

¹⁸⁷ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa374909\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa374909(v=vs.85).aspx)

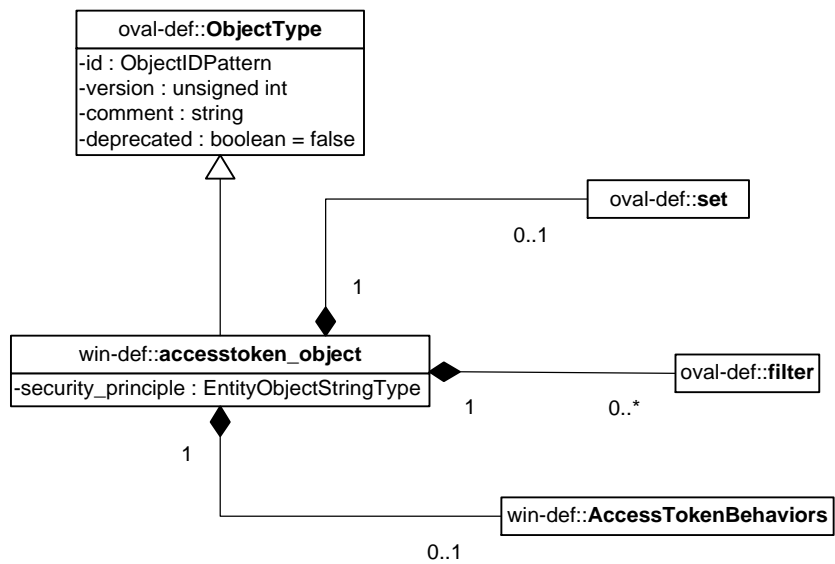
2.34.1. Known Supported Platforms

- Windows XP
- Windows Vista
- Windows 7

2.35. win-def:accesstoken_object

The `accesstoken_object` construct defines the security principal that identifies user, group, or computer account associated with an access token¹⁸⁸, whose associated information should be collected and represented as `accesstoken_items`.

This object has been deprecated and will be removed in version 6.0 of the language. Due to scalability issues, it is encouraged that you use the `userright_object`.



Property	Type	Multiplicity	Nullable	Description
set	oval-def:set	0..1	false	Enables the expression of complex <code>accesstoken_objects</code> that are the result of logically combining and filtering the <code>accesstoken_items</code> that are identified by one or more <code>accesstoken_objects</code> .
behaviors	win-def: AccesstokenBehaviors	0..1	false	Specifies the behaviors that direct how the <code>accesstoken_object</code> collects <code>accesstoken</code>

¹⁸⁸ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms677942\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms677942(v=vs.85).aspx)

				<code>items</code> 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 <code>accesstoken_items</code> from the set of <code>accesstoken_items</code> collected by a <code>accesstoken_object</code> . Please see the OVAL Language Specification [2] for additional information.

2.36. 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.

This behavior has been deprecated and will be removed in version 6.0 of the language. Due to scalability issues, it is encouraged that you use the `userright_test`.

Attribute	Type	Possible Values	Description
include_group	bool	<i>'true'</i> <i>'false'</i>	Defines whether or not the group SID should be collected when the <code>trustee_sid</code> property specifies a group SID. <i>'true'</i> : The group SID

			<p><u>MUST</u> be collected when the trustee_sid property specifies a group SID.</p> <p><i>'false'</i>: The group SID <u>MUST NOT</u> be collected when the trustee_sid property specifies a group SID.</p> <p>Default Value: true</p>
resolve_group	bool	<p><i>'true'</i></p> <p><i>'false'</i></p>	<p>Defines whether or not the members of group SIDs should be resolved and collected.</p> <p>Note that all child groups should also be resolved and any valid domain accounts that are members should also be included.</p> <p>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.</p> <p><i>'true'</i>: The members of a group SID <u>MUST</u> be resolved and collected.</p> <p><i>'false'</i>: The members of a group SID <u>MUST NOT</u> be resolved or collected.</p> <p>Default Value: false</p>

2.37. 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 privileges¹⁸⁹, and all attributes ending in "right", with the exception of `settrustedcredmanaccessnameright`, which is a privilege¹⁹⁰, are access token rights¹⁹¹.

This state has been deprecated and will be removed in version 6.0 of the language. Due to scalability issues, it is encouraged that you use the `userright_state`.

¹⁸⁹ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/bb530716\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/bb530716(v=vs.85).aspx)

¹⁹⁰ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/bb530716\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/bb530716(v=vs.85).aspx)

¹⁹¹ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/bb545671\(v=VS.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/bb545671(v=VS.85).aspx)



Property	Type	Multiplicity	Nullable	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.
seenabledlegationprivilege	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.
seremotesutdownprivilege	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.
setrustrustedcredmanageraccessnameright	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_ACC

				ESS_NAME), not a right.
--	--	--	--	-------------------------

2.38. 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 privileges¹⁹², and all attributes ending in "right", with the exception of `settrustedcredmanaccessnameright`, which is a privilege¹⁹³, are access token rights¹⁹⁴.

This item has been deprecated and will be removed in version 6.0 of the language. Due to scalability issues, it is encouraged that you use the `userright_item`.

¹⁹² For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/bb530716\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/bb530716(v=vs.85).aspx)

¹⁹³ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/bb530716\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/bb530716(v=vs.85).aspx)

¹⁹⁴ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/bb545671\(v=VS.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/bb545671(v=VS.85).aspx)



Property	Type	Multiplicity	Nilable	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

				<p>accounts, and computer accounts created when a computer joins a domain.</p> <p>In Windows, security principals are case-insensitive. As a result, it is recommended that the case-insensitive operations are used for this entity.</p>
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.
seenabledelegation	oval-sc:EntityItemBoolType	0..1	false	Gives the user the privilege to

privilege				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.
seprofilesinglprocessprivilege	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.
seremotesutdownprivilege	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.
sesutdownprivilege	oval-sc:EntityItemBoolType	0..1	false	Gives the user the privilege to

e				shut down the system.
sesyncagentprivilege	oval-sc:EntityItemBoolType	0..1	false	<p>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.</p> <p>By default, it is assigned to the Administrator and LocalSystem accounts on domain controllers.</p>
sesystemenvironmentprivilege	oval-sc:EntityItemBoolType	0..1	false	<p>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.</p>
sesystemprofileprivilege	oval-sc:EntityItemBoolType	0..1	false	<p>Gives the user the privilege to profile system performance.</p>
sesystemtimeprivilege	oval-sc:EntityItemBoolType	0..1	false	<p>Gives the user the privilege to change the system time.</p>
setakeownershipprivilege	oval-sc:EntityItemBoolType	0..1	false	<p>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.</p>
setcbprivilege	oval-sc:EntityItemBoolType	0..1	false	<p>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.</p>
setimezoneprivilege	oval-sc:EntityItemBoolType	0..1	false	<p>Gives the user the privilege to change the time zone.</p>
seundockprivilege	oval-sc:EntityItemBoolType	0..1	false	<p>Gives the user the privilege to remove the computer from a docking station.</p>
seunsolicitedinputprivilege	oval-sc:EntityItemBoolType	0..1	false	<p>Allows the user to read unsolicited input from a</p>

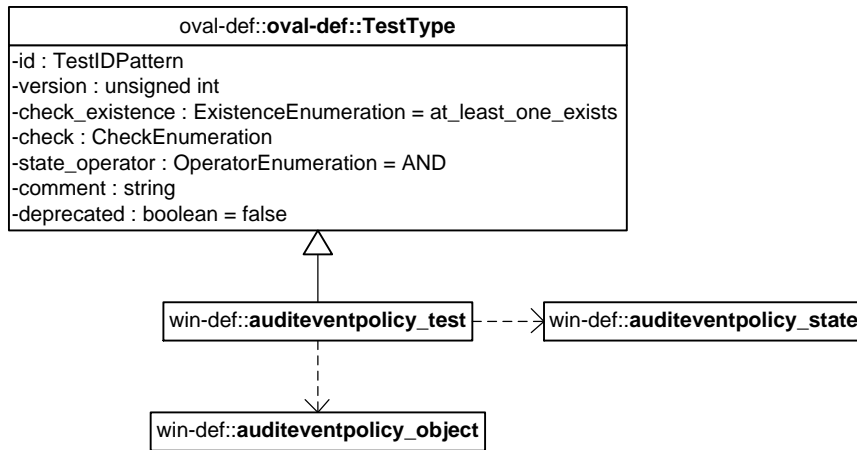
				terminal device.
sebatchlogonright	oval-sc:EntityItemBoolType	0..1	false	Grants the right for an account to log on using the batch logon type.
seinteractivelogonright	oval-sc:EntityItemBoolType	0..1	false	Grants the right for an account to log on using the interactive logon type.
senetworklogonright	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.
sedeny Servicelogonright	oval-sc:EntityItemBoolType	0..1	false	Denies the right for an account to log on using the service logon type.
setrustrustedcredmanacccessnameright	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.

2.39. win-def:auditeventpolicy_test

The `auditeventpolicy_test` is used to make assertions about the different types of events the system should audit¹⁹⁵. The `auditeventpolicy_test` MUST reference one

¹⁹⁵ For more information see [http://technet.microsoft.com/en-us/library/cc766468\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc766468(WS.10).aspx)

`auditeventpolicy_object` and zero or more `auditeventpolicy_states`.

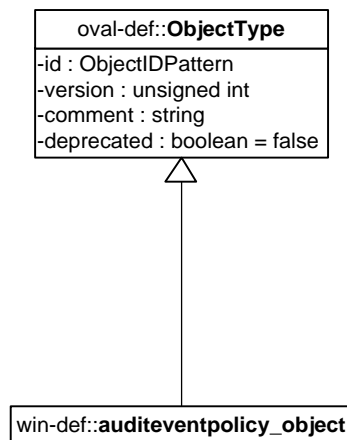


2.39.1. Known Supported Platforms

- Windows XP
- Windows Vista
- Windows 7

2.40. win-def:auditeventpolicy_object

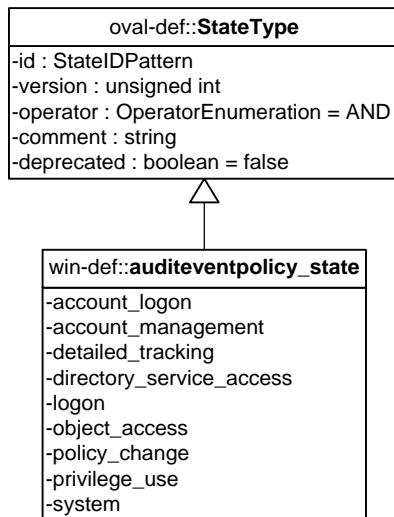
The `auditeventpolicy_object` construct defines the set of audit events whose associated information should be collected and represented as `auditeventpolicy_items`. Because there is only one object relating to audit event policy (the system as a whole), there are no child entities defined for this object,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



2.41. 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.



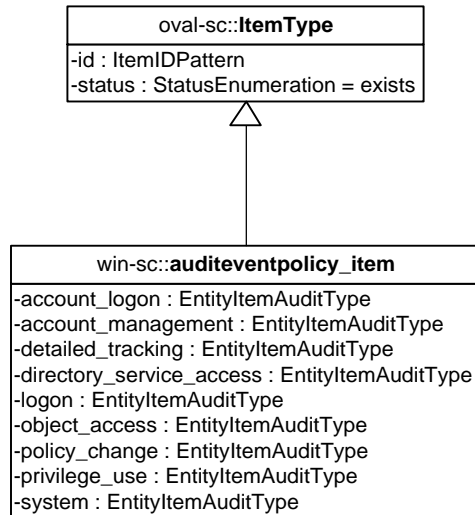
Property	Type	Multiplicity	Nullable	Description
account_logon	win-def: EntityStateAuditType	0..1	false	The OS MUST audit each instance of a user attempt to log on or log off this computer, as well as audit logon attempts by privileged accounts that log on to the domain controller.
account_management	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-	0..1	false	The OS MUST audit each time

¹⁹⁶ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms721903\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms721903(v=vs.85).aspx)

	def:EntityStateAuditType			this computer validates the credentials of an account.
object_access	win-def: EntityStateAuditType	0..1	false	<p>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.</p> <p>The type of access request, such as Write, Read, or Modify, and the account making the request MUST match the settings in the SACL.</p>
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	<p>The OS must audit attempts to change the system time, startup, restart, or shutdown the system, and load extensible authentication features.</p> <p>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.</p>

2.42. 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.



Property	Type	Multiplicity	Nilable	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

¹⁹⁷ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms721903\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms721903(v=vs.85).aspx)

				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.

2.43. 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.

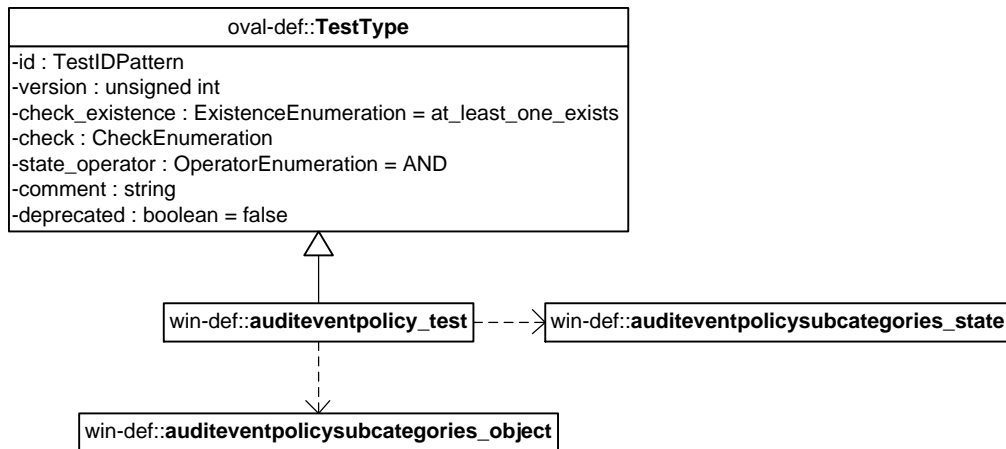
2.44. win-sc:EntityItemAuditType

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.

2.45. win-def:auditeventpolicysubcategories_test

The `auditeventpolicysubcategories_test` is used to make assertions about the different audit event policy settings on a Windows system¹⁹⁸. The `auditeventpolicysubcategories_test` MUST reference one `auditeventpolicysubcategories_object` and zero or more `auditeventpolicysubcategories_states`.



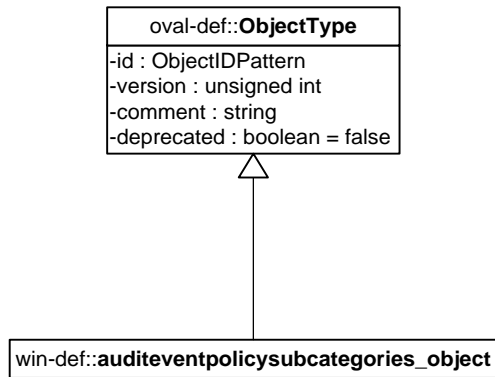
2.45.1. Known Supported Platforms

- Windows XP
- Windows Vista
- Windows 7 (not guaranteed for the `kerberos_ticket_events` category)

2.46. 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.

¹⁹⁸ For more information see [http://msdn.microsoft.com/en-us/library/dd976913\(v=PROT.10\).aspx](http://msdn.microsoft.com/en-us/library/dd976913(v=PROT.10).aspx)



2.47. 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 platforms¹⁹⁹.

¹⁹⁹ For more information see [http://msdn.microsoft.com/en-us/library/dd973928\(v=PROT.10\).aspx](http://msdn.microsoft.com/en-us/library/dd973928(v=PROT.10).aspx)



Property	Type	Multiplicity	Nilable	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
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

²⁰⁰ For more information see [http://technet.microsoft.com/en-us/library/cc766468\(W.S.10\).aspx](http://technet.microsoft.com/en-us/library/cc766468(W.S.10).aspx)

				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 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

²⁰¹ For more information see [http://msdn.microsoft.com/en-us/library/Oe57a2df-f576-4f59-8c6e-9515567f9900\(v=PROT.10\)#ad_ds](http://msdn.microsoft.com/en-us/library/Oe57a2df-f576-4f59-8c6e-9515567f9900(v=PROT.10)#ad_ds)

				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_ser	win-def:	0..1	false	The OS must audit events

ver	EntityStateAuditType			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	<p>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.</p> <p>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.</p> <p>Enabling Handle Manipulation causes implementation-specific security event data to be logged identifying the permissions that were used to grant or deny the access</p>

				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: <ul style="list-style-type: none"> - 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}.

2.48. win-sc:auditeventpolicysubcategories_item

The `auditeventpolicysubcategories_item` construct stores the different subcategories of event types the system should audit²⁰².

²⁰² For more information see [http://msdn.microsoft.com/en-us/library/dd973928\(v=PROT.10\).aspx](http://msdn.microsoft.com/en-us/library/dd973928(v=PROT.10).aspx)



Property	Type	Multi- city	Null- able	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
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

²⁰³ For more information see [http://technet.microsoft.com/en-us/library/cc766468\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc766468(WS.10).aspx)

				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 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

²⁰⁴ For more information see [http://msdn.microsoft.com/en-us/library/0e57a2df-f576-4f59-8c6e-9515567f9900\(v=PROT.10\)#ad_ds](http://msdn.microsoft.com/en-us/library/0e57a2df-f576-4f59-8c6e-9515567f9900(v=PROT.10)#ad_ds)

				{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	<p>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.</p> <p>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.</p> <p>Enabling Handle Manipulation causes implementation-specific security event data to be logged identifying the permissions that were used</p>

				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: <ul style="list-style-type: none"> - 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}.

2.49. 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.

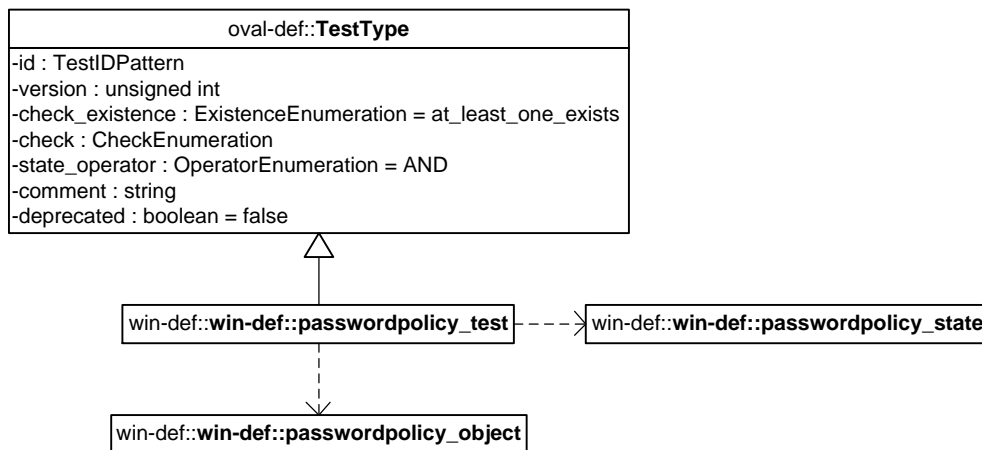
2.50. win-sc:EntityItemAuditType

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.

2.51. win-def:passwordpolicy_test

The `passwordpolicy_test` is used to check specific policies associated with passwords on Windows based systems²⁰⁵. 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`.



2.51.1. Known Supported Platforms

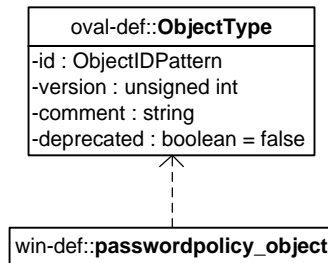
- Windows XP
- Windows Vista
- Windows 7

2.52. 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

²⁰⁵ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms721882\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms721882(v=vs.85).aspx)

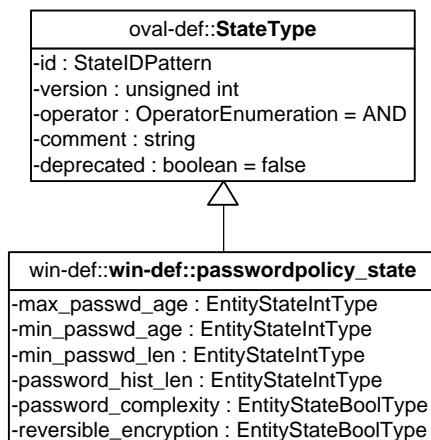
there is only one object relating to password policy (the system as a whole), there are no child entities defined for this object, so it is considered empty.



2.53. 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 platforms²⁰⁶.

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 int²⁰⁷.



Property	Type	Multiplicity	Nullable	Description
<code>max_passwd_age</code>	oval-def:EntityStateIntType	0..1	false	Alternate name: "Maximum password age." Determines the period (in seconds) that a

²⁰⁶ For more information see <http://msdn.microsoft.com/en-us/library/ms878685.aspx>

²⁰⁷ For more information see line 110 of http://doxygen.reactos.org/da/d6c/lmaccess_8h_source.html

				<p>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.</p> <p>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).</p>
min_passwd_age	oval-def:EntityStateIntType	0..1	false	<p>Alternate name: "Minimum password age." Determines the period (in seconds) that a password must be used before the user can change it.</p> <p>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.</p> <p>The default in the Default Domain GPO, as well as workstations and servers, is 0.</p>
min_passwd_len	oval-def:EntityStateIntType	0..1	false	<p>Alternate name: "Minimum password length." Determines the least number of characters a user account's password may contain.</p> <p>In OVAL, values range from 0 to 14 inclusive, where 0 indicates that no password is</p>

				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	<p>Alternate name: "Enforce password history."</p> <p>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.</p>
password_complexity	oval-def:EntityStateBoolType	0..1	false	<p>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.</p> <p>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.</p> <p>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</p>

				0 in OVAL.
reversible_encryption	oval-def: EntityStateBoolType	0..1	false	<p>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.</p> <p>This determines whether Windows will store passwords using reversible encryption.</p> <p>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.</p> <p>The default in the Default Domain GPO, as well as workstations and servers, is "Disabled," or 0 in OVAL.</p>

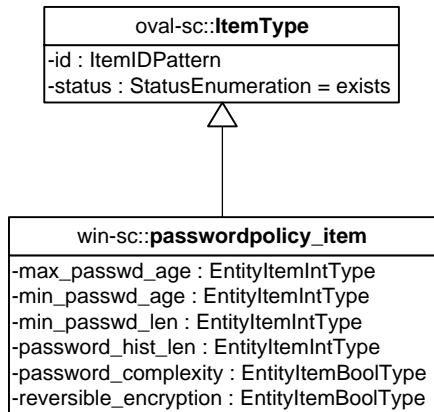
2.54. win-sc:passwordpolicy_item

The `passwordpolicy_item` construct stores the different policies on password that should be collected²⁰⁸.

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 int²⁰⁹.

²⁰⁸ For more information see <http://msdn.microsoft.com/en-us/library/ms878685.aspx>

²⁰⁹ For more information see line 110 of http://doxygen.reactos.org/da/d6c/lmaccess_8h_source.html



Property	Type	Multiplicity	Nullable	Description
max_passwd_age	oval-def:EntityItemIntType	0..1	false	<p>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.</p> <p>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.</p> <p>In addition, max_passwd_age can take on the value of TIMEQ_FOREVER to indicate that passwords NEVER expire.</p> <p>The default in the Default Domain Group Policy Object (GPO), as well as workstations and servers is 42*86400 = 3628800 (42 days).</p>
min_passwd_age	oval-def:EntityItemIntType	0..1	false	<p>Alternate name: "Minimum password age." Determines the period (in seconds) that a password must be used before the user can change it.</p> <p>In OVAL, values range from 0</p>

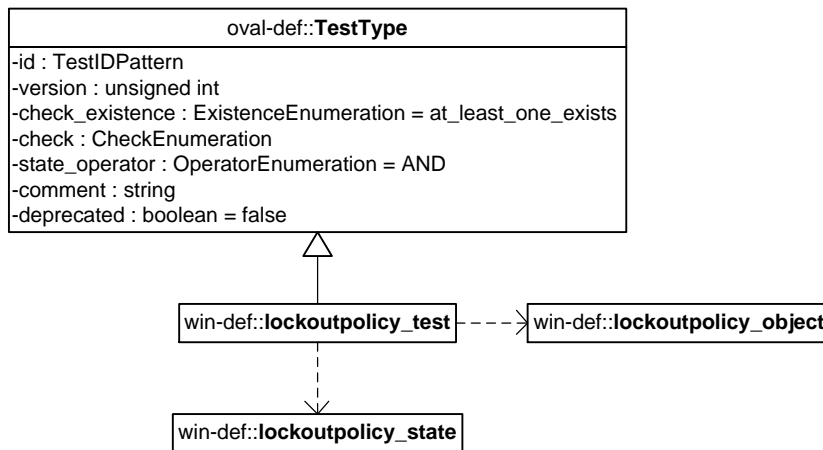
				<p>* 86400 (changes can happen immediately) to 999 * 86400 = 86313600 (999 days) inclusive, where 86400 is the number of seconds in one day.</p> <p>The default in the Default Domain GPO, as well as workstations and servers, is 0.</p>
min_passwd_len	oval-def:EntityItemIntType	0..1	false	<p>Alternate name: "Minimum password length." Determines the least number of characters a user account's password may contain.</p> <p>In OVAL, values range from 0 to 14 inclusive, where 0 indicates that no password is required.</p> <p>The default in the Default Domain GPO, as well as workstations and servers, is 0.</p>
password_hist_len	oval-def:EntityItemIntType	0..1	false	<p>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.</p> <p>Values range from 0 to 24 inclusive. The default in the Default Domain GPO, as well as workstations and servers, is 1.</p>
password_complexity	oval-def:EntityItemBoolType	0..1	false	<p>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.</p>

			<p>This attribute determines whether passwords meet complexity requirements.</p> <p>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.</p> <p>Complexity requirements are enforced upon password change or creation.</p> <p>The default in the Default Domain GPO, as well as workstations and servers, is "Disabled," or 0 in OVAL.</p>
<p>reversible_encryption</p>	<p>oval-def: EntityItemBoolType</p>	<p>0..1</p>	<p>false</p> <p>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.</p> <p>This determines whether Windows will store passwords using reversible encryption.</p> <p>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</p>

			<p>need to protect password information.</p> <p>The default in the Default Domain GPO, as well as workstations and servers, is "Disabled," or 0 in OVAL.</p>
--	--	--	--------------------------------------------------------------------------------------------------------------------------------------------------------------

2.55. win-def:lockoutpolicy_test

The `lockoutpolicy_test` is used to make assertions about with lockout information for users and global groups in the security database²¹⁰. The `lockoutpolicy_test` MUST reference one `lockoutpolicy_object` and zero or more `lockoutpolicy_states`.



2.55.1. Known Supported Platforms

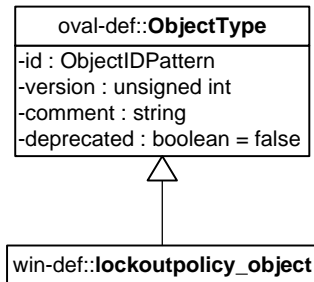
- Windows XP
- Windows Vista
- Windows 7

2.56. 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

²¹⁰ For more information about the various tools for lockout policies see [http://technet.microsoft.com/en-us/library/cc738772\(WS.10\).aspx](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>

lockoutpolicy_items²¹¹. 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.



2.57. 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 platforms²¹². 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. 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

²¹¹ For more information about the various tools for lockout policies see

[http://technet.microsoft.com/en-us/library/cc738772\(WS.10\).aspx](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>

²¹² For more information about the various tools for lockout policies see [http://technet.microsoft.com/en-us/library/cc738772\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc738772(WS.10).aspx)

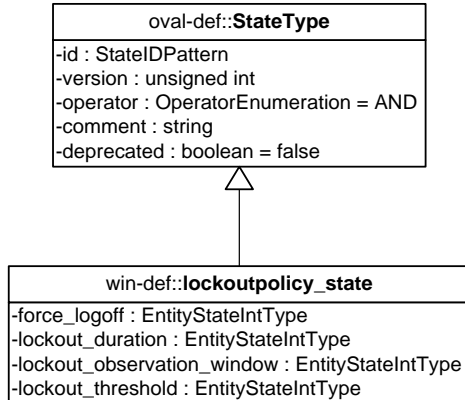
For more information about lockout policies in general see

<http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=6218>

²¹³ For more information about the properties in `lockoutpolicy_state` see

<http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=6218>

TIMEQ_FOREVER is defined as the value of -1, cast as an unsigned int²¹⁴.



Property	Type	Multiplicity	Nilable	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	<p>Alternate name: "Account lockout duration." Determines the number of SECONDS a locked-out account remains locked out before automatically becoming unlocked.</p> <p>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.</p> <p>If you set the account lockout duration to TIMEQ_FOREVER, the account MUST be locked</p>

²¹⁴ For more information see line 110 of http://doxygen.reactos.org/da/d6c/lmaccess_8h_source.html

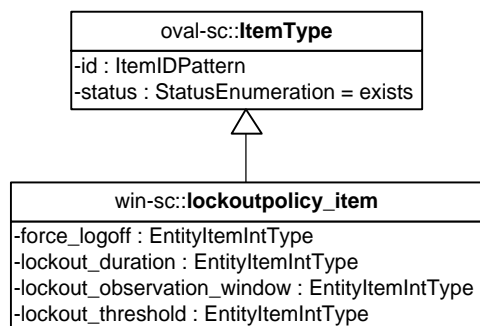
				<p>out until an administrator explicitly unlocks it²¹⁵. This policy on has meaning when Account lockout threshold is specified.</p> <p>The default value is $30 * 60 = 1800$ (30 minutes).</p>
lockout_observation_window	oval-def:EntityStateIntType	0..1	false	<p>Indicates the amount of time in SECONDS in which failed password attempts are counted without resetting the count to zero.</p> <p>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).</p>
lockout_threshold	oval-def:EntityStateIntType	0..1	false	<p>Alternate name: "Account lockout threshold." Determines the number of failed logon attempts that will cause a user account to be locked out.</p> <p>A locked out account cannot be used until it is reset by an administrator or the account lockout duration has expired.</p> <p>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.</p> <p>By default, this setting is 0 in the Default Domain Group Policy object (GPO) and in the</p>

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](http://msdn.microsoft.com/en-us/library/windows/desktop/aa371355(v=vs.85).aspx)

				local security policy of workstations and servers.
--	--	--	--	----------------------------------------------------

2.58. win-sc: lockoutpolicy_item

The `lockoutpolicy_item` enumerates various attributes associated with lockout information for users and global groups in the security database.



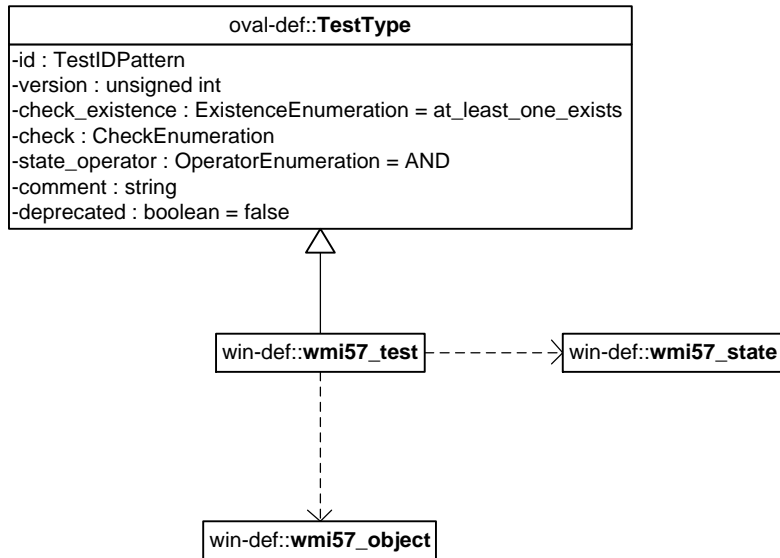
Property	Type	Multiplicity	Nullable	Description
force_logoff	oval-def:EntityStateIntType	0..1	false	Indicates the amount of time in SECONDS (not MINUTES) that an interactive logon session is allowed to continue.
lockout_duration	oval-def:EntityStateIntType	0..1	false	<p>Alternate name: "Account lockout duration."</p> <p>Determines the number of SECONDS a locked-out account remains locked out before automatically becoming unlocked.</p> <p>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.</p> <p>If you set the account lockout duration to TIMEQ_FOREVER, the account MUST be locked out until an administrator</p>

				explicitly unlocks it 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	<p>Indicates the amount of time in SECONDS in which failed password attempts are counted without resetting the count to zero.</p> <p>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).</p>
lockout_threshold	oval-def:EntityStateIntType	0..1	false	<p>Alternate name: "Account lockout threshold." Determines the number of failed logon attempts that will cause a user account to be locked out.</p> <p>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.</p> <p>By default, this setting is 0 in the Default Domain Group Policy object (GPO) and in the local security policy of workstations and servers.</p>

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](http://msdn.microsoft.com/en-us/library/windows/desktop/aa371355(v=vs.85).aspx)

2.59. win-def:wmi57_test

The `wmi57_test` is used to make assertions about information accessed by WMI²¹⁷. The `wmi57_test` MUST reference one `wmi57_object` and zero or more `wmi57_states`.



2.59.1. Known Supported Platforms

- Windows XP
- Windows Vista
- Windows 7

2.60. win-def:wmi57_object

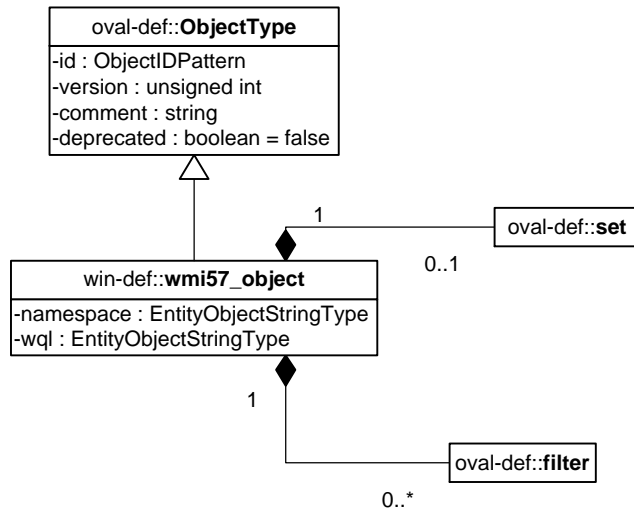
The `wmi57_object` construct defines the applicable WMI information that should be collected and represented as `wmi57_items`²¹⁸.

²¹⁷ For more information see

<http://msdn.microsoft.com/en-us/library/windows/desktop/aa394582%28v=vs.85%29.aspx>

²¹⁸ For more information see

<http://msdn.microsoft.com/en-us/library/windows/desktop/aa394582%28v=vs.85%29.aspx>



Property	Type	Multiplicity	Nullable	Description
set	oval-def:set	0..1	false	Enables the expression of complex <code>wmi57_objects</code> that are the result of logically combining and filtering the <code>wmi57_items</code> that are identified by one or more <code>wmi57_objects</code> .
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 .
wql	oval-def:EntityObjectStringType	0..1	false	A WQL query used to identify the <code>wmi57_objects</code> to represent as <code>wmi57_items</code> . Any valid WQL query is usable with one exception, all fields must be named in the SELECT portion of the query ²²⁰ .
filter	oval-def:filter [2]	0..*	false	Allows for the explicit

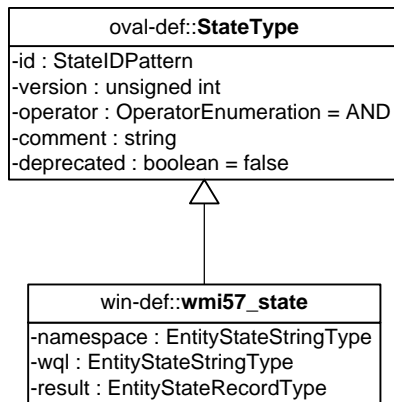
²¹⁹ For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa394582%28v=vs.85%29.aspx>

²²⁰ For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa394606%28v=vs.85%29.aspx>

				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.
--	--	--	--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------

2.61. 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 platforms²²¹.



Property	Type	Multiplicity	Nullable	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 .
wql	oval-def:	0..1	false	A WQL query used to identify

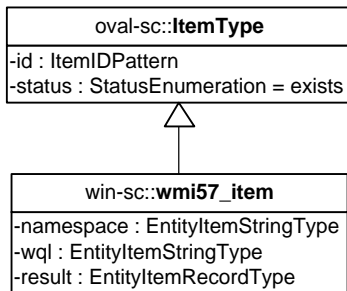
²²¹ For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa394582%28v=vs.85%29.aspx>

²²² For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa394582%28v=vs.85%29.aspx>

	EntityStateStringType			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 .
result	oval-def: EntityStateRecordType	0..1	false	The result attribute specifies how to test items in the result set of the specified WQL statement.

2.62. win-sc:wmi57_item

The wmi57_item outlines information to be checked through Microsoft's WMI interface.



Property	Type	Multipl city	Nilla ble	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 .
wql	oval-sc:EntityItemStringType	0..1	false	A WQL query used to identify the wmi57_objects to

²²³ For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa394606%28v=vs.85%29.aspx>

²²⁴ For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa394582%28v=vs.85%29.aspx>

				represent as <code>wmi57_items</code> . Any valid WQL query is usable with one exception, all fields must be named in the SELECT portion of the query ²²⁵ .
result	oval-sc: EntityItemRecordType	0..*	false	The result attribute specifies how to test items in the result set of the specified WQL statement.

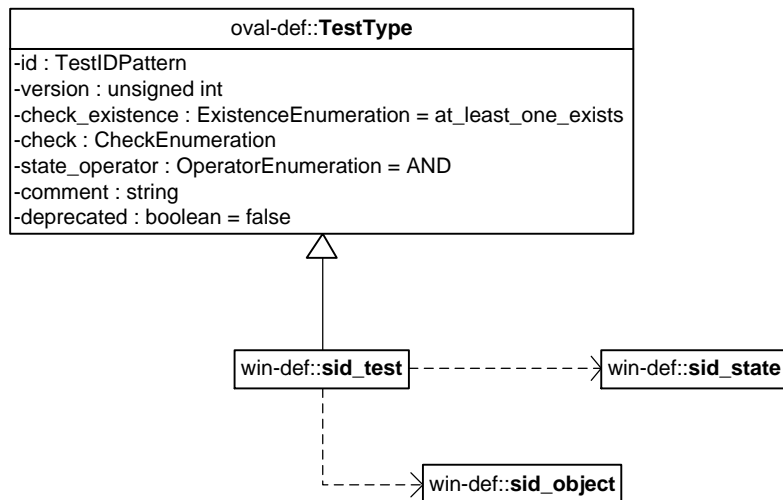
2.63. win-def:sid_test

The `sid_test` is used to make assertions about the properties associated with the specified trustee²²⁶ name and its corresponding SID²²⁷. 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`.

²²⁵ For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa394606%28v=vs.85%29.aspx>

²²⁶ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379637\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379637(v=vs.85).aspx)

²²⁷ For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379571%28v=vs.85%29.aspx>



2.63.1. Known Supported Platforms

- Windows XP
- Windows Vista
- Windows 7

2.64. win-def:sid_object

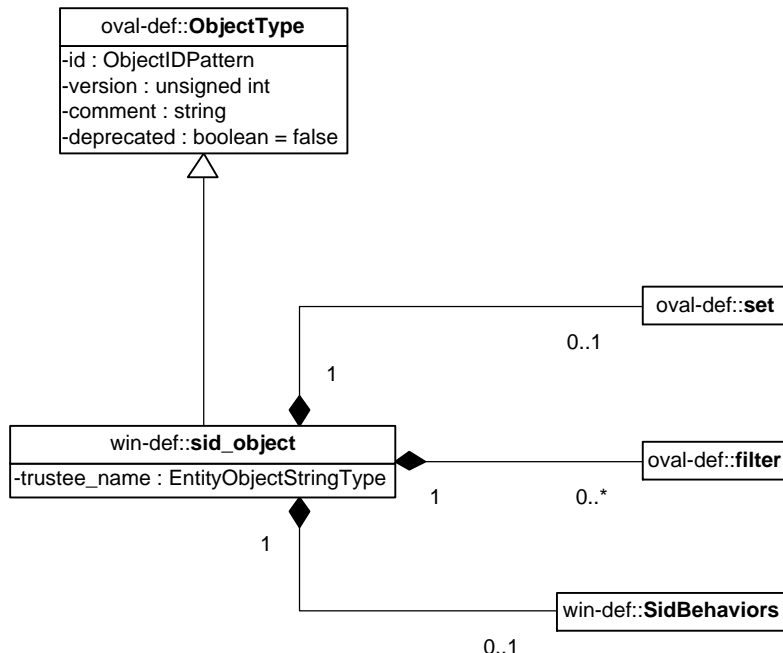
The `sid_object` construct defines the object set, in this case a set of SIDs (identified by name), whose associated information should be collected and represented as `sid_items`²²⁸.

²²⁸ For more information about trustees see

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



Property	Type	Multiplicity	Nullable	Description
set	oval-def:set	0..1	false	Enables the expression of complex <code>sid_objects</code> that are the result of logically combining and filtering the <code>sid_items</code> that are identified by one or more <code>sid_objects</code> .
behavior	win-def:SidBehaviors	0..1	false	Specifies the behaviors that direct how the <code>sid_object</code> collects <code>sid_items</code> from the system.
trustee_name	oval-def:EntityObjectStringType	1..1	false	The <code>trustee_name</code> 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 .

²²⁹ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379637\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379637(v=vs.85).aspx)

				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 .
filter	oval-def:filter [2]	0..*	false	Allows for the explicit inclusion or exclusion of <code>sid_items</code> from the set of <code>sid_items</code> collected by a <code>sid_object</code> . Please see the OVAL Language Specification [2] for additional information.

2.65. 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.

²³⁰ For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379159%28v=VS.85%29.aspx>

			Default Value: true
resolve_group	bool	'true' 'false'	<p>Defines whether or not the members of group SIDs should be resolved and collected.</p> <p>Note that all child groups should also be resolved and any valid domain accounts that are members should also be included.</p> <p>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.</p> <p>'true': The members of a group SID <u>MUST</u> be resolved and collected.</p> <p>'false': The members of a group SID <u>MUST NOT</u> be resolved or collected.</p> <p>Default Value: false</p>

2.66. win-def:sid_state

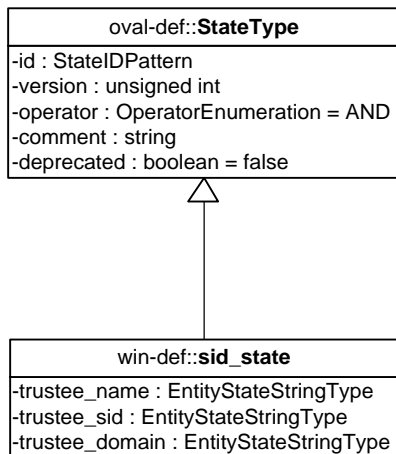
The `sid_state` construct is used by a `sid_test` to specify the different rights that can be associated with a given `sid_object` under Microsoft Windows platforms²³¹.

²³¹ For more information about trustees see

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



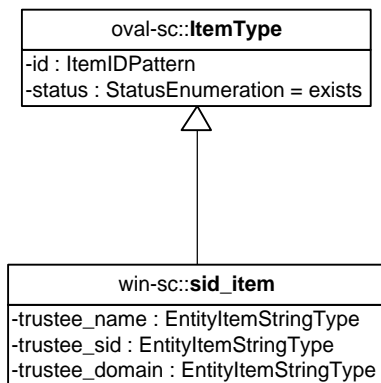
Property	Type	Multiplicity	Nullable	Description
trustee_name	oval-def: EntityStateStringType	0..1	false	<p>The trustee_name property is the unique name (case-insensitive in Windows) that is associated to a particular SID.</p> <p>A SID can be associated with a user, group, or program (such as a Windows service). Because trustee names are case-insensitive, it is recommended that the case-insensitive operations are used for this attribute²³².</p> <p>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</p>

²³² For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379637\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379637(v=vs.85).aspx)

				the trustee name without a domain 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.

2.67. win-sc:sid_item

The `sid_item` stores the attributes associated with a given `sid_object` under Microsoft Windows platforms.



Property	Type	Multipli city	Nilla ble	Description
trustee_name	oval-sc:EntityItemStringType	0..1	false	<p>The <code>trustee_name</code> property is the unique name (case-insensitive in Windows) that is associated to a particular SID.</p> <p>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-</p>

²³³ For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379159%28v=VS.85%29.aspx>

				insensitive operations are used for this attribute 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 .
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.

2.68. win-def:sid_sid_test

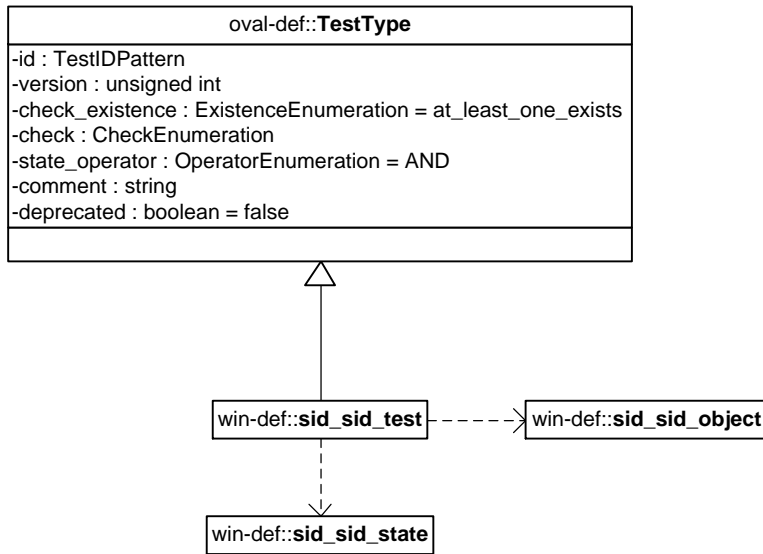
The `sid_sid_test` is used to check properties associated with the specified SID. Note that this test was added in version 5.4 as a temporary fix. There is a need within the community to identify objects like users and groups by both the name²³⁶ and the SID²³⁷. The `sid_test` should be used instead when the object is identified by name. The `sid_sid_test` MUST reference one `sid_sid_object` and zero or more `sid_sid_states`.

²³⁴ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379637\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379637(v=vs.85).aspx)

²³⁵ For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379159%28v=VS.85%29.aspx>

²³⁶ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379637\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379637(v=vs.85).aspx)

²³⁷ For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379571%28v=vs.85%29.aspx>

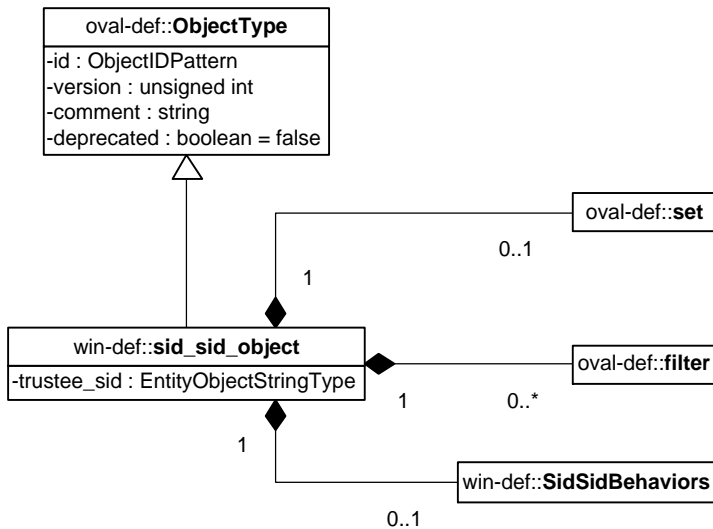


2.68.1. Known Supported Platforms

- Windows XP
- Windows Vista
- Windows 7

2.69. 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	Nullable	Description
set	oval-def:set	0..1	false	Enables the expression of complex <code>sid_sid_objects</code> that are the result of logically combining and filtering the <code>sid_sid_items</code> that are identified by one or more <code>sid_sid_objects</code> .
behavior	win-def:SidSidBehaviors	0..1	false	Specifies the behaviors that direct how the <code>sid_sid_object</code> collects <code>sid_sid_items</code> 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 .
filter	oval-def:filter [2]	0..*	false	Allows for the explicit inclusion or exclusion of <code>sid_sid_items</code> from the set of <code>sid_sid_items</code> collected by a <code>sid_sid_object</code> . Please see the OVAL Language Specification [2] for additional information.

2.70. 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.

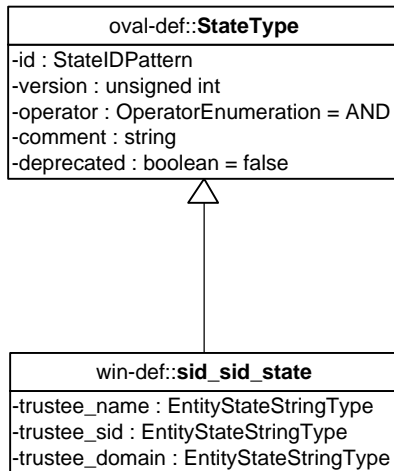
Attribute	Type	Possible Values	Description
include_group	boolean	'true' 'false'	Defines whether or not the group SID should be collected when the <code>trustee_sid</code> property specifies a group SID. 'true': The group SID MUST be collected when the <code>trustee_sid</code> property specifies a group SID.

²³⁸ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379166\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379166(v=vs.85).aspx)

			<p><i>'false'</i>: The group SID MUST NOT be collected when the trustee_sid property specifies a group SID.</p> <p>Default Value: true</p>
resolve_group	boolean	<p><i>'true'</i></p> <p><i>'false'</i></p>	<p>Defines whether or not the members of group SIDs should be resolved and collected.</p> <p>Note that all child groups should also be resolved and any valid domain accounts that are members should also be included.</p> <p>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.</p> <p><i>'true'</i>: The members of a group SID MUST be resolved and collected.</p> <p><i>'false'</i>: The members of a group SID MUST NOT be resolved or collected.</p> <p>Default Value: false</p>

2.71. 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.



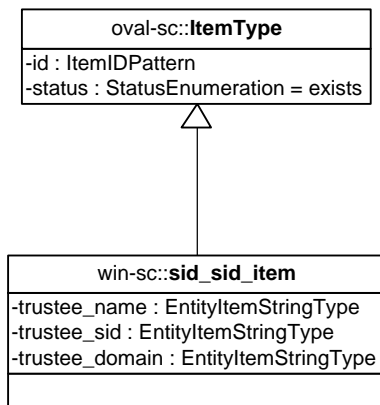
Property	Type	Multiplicity	Nullable	Description
trustee_name	oval-def: EntityStateStringType	0..1	false	<p>The trustee_name property is the unique name (case-insensitive in Windows) that is associated to a particular SID. A SID can be associated with a user, group, or program (such as a Windows service).</p> <p>Because trustee names are case-insensitive, it is recommended that the case-insensitive operations are used for this property²³⁹.</p> <p>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</p>

²³⁹ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379637\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379637(v=vs.85).aspx)

				the trustee name without a domain 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.

2.72. 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	Nullable	Description
trustee_name	oval-sc: EntityItemStringType	0..1	false	<p>The <code>trustee_name</code> 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).</p> <p>Because trustee names are case-insensitive, it is recommended that the case-insensitive operations are used for this property²⁴¹.</p>

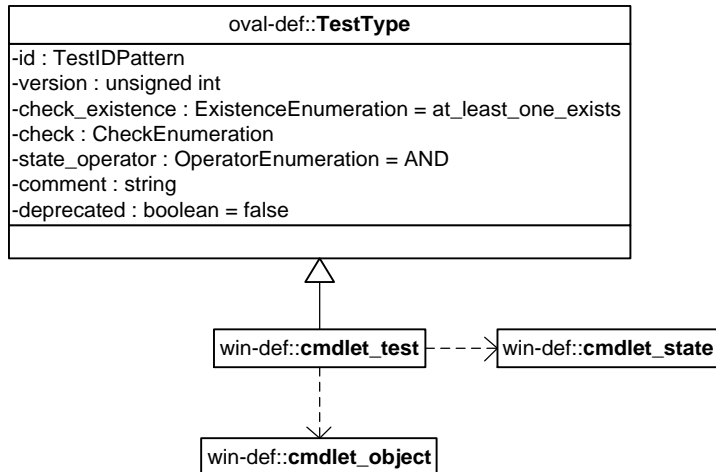
²⁴⁰ For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379159%28v=VS.85%29.aspx>

²⁴¹ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa379637\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379637(v=vs.85).aspx)

				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 .
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.

2.73. 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.



2.73.1. Known Supported Platforms

- Windows XP
- Windows Vista
- Windows 7

²⁴² For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa379159%28v=VS.85%29.aspx>

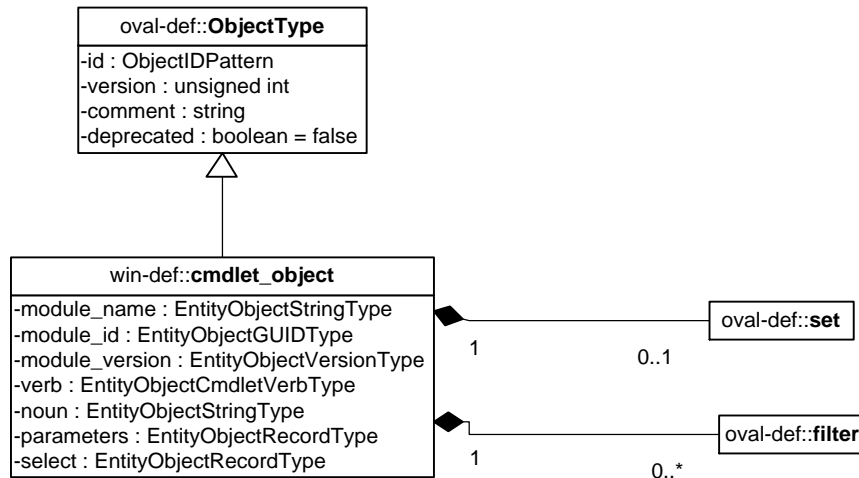
²⁴³ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms714395\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms714395(v=vs.85).aspx)

2.74. 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.

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 Concepts²⁴⁵. Certain attributes (such as nouns, verbs, and parameter names) SHOULD align with the MSDN documentation²⁴⁶.

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` enumeration²⁴⁷.



²⁴⁴ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms714395\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms714395(v=vs.85).aspx)

²⁴⁵ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ee706608\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ee706608(v=vs.85).aspx)

²⁴⁶ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms714423\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms714423(v=vs.85).aspx)

²⁴⁷ For more information see <http://msdn.microsoft.com/en-us/library/system.management.automation.pslanguagemode.aspx>

Property	Type	Multiplicity	Nullable	Description
set	oval-def:set	0..1	false	Enables the expression of complex <code>cmdlet_objects</code> that are the result of logically combining and filtering the <code>cmdlet_items</code> that are identified by one or more <code>cmdlet_objects</code> .
module_name	oval-def:EntityObjectStringType	1..1	true	The name of the module that defines the <code>cmdlet</code> ²⁴⁸ . When set using the <code>New-Module</code> command in Powershell, the default name is <code>__DynamicModule_PATHID</code> where "PATHID" is a unique identifier that specifies the path to the dynamic module ²⁴⁹ . If <code>xsi:nil="true"</code> , 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 . If <code>xsi:nil="true"</code> , it implies that it does not matter which module GUID the command comes from.

²⁴⁸ For more information see <http://www.microsoft.com/download/en/details.aspx?id=9706>

²⁴⁹ For more information see <http://technet.microsoft.com/en-us/library/dd819471.aspx>

²⁵⁰ For more information see the examples in <http://technet.microsoft.com/en-us/library/dd819471.aspx>

module_version	oval-def: EntityObjectVersionType	1..1	true	Module version in the format of MAJOR.MINOR 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 . This verb specifies the action ²⁵³ taken by the cmdlet. NOTE: In Windows Powershell, verbs describe a word that <i>implies</i> an action even if that word is not a standard verb in the English language, such as <i>New</i> .
noun	oval-def: EntityObjectStringType	1..1	false	The noun name of the cmdlet ²⁵⁴ . This noun specifies the resource 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 . Also, parameter names SHOULD align with the MSDN documentation ²⁵⁷ .
select	oval-def: EntityObjectRecordType	0..1	true	A set of name and value pairs used as input to the Select-Object ²⁵⁸ cmdlet in order to

²⁵¹ For more information see the examples in <http://technet.microsoft.com/en-us/library/dd819471.aspx>

²⁵² For more information see <http://www.microsoft.com/download/en/details.aspx?id=9706>

²⁵³ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms714428\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms714428(v=vs.85).aspx)

²⁵⁴ For more information see <http://www.microsoft.com/download/en/details.aspx?id=9706>

²⁵⁵ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms714423\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms714423(v=vs.85).aspx)

²⁵⁶ For more information see <http://www.microsoft.com/download/en/details.aspx?id=9706>

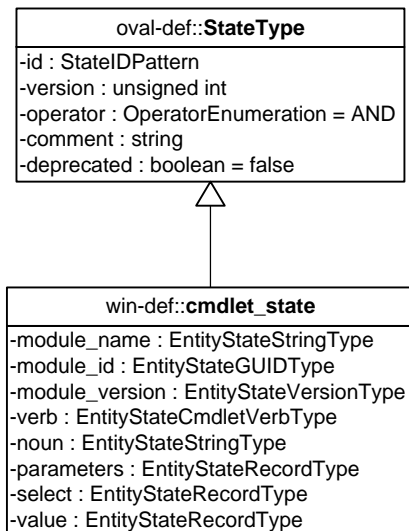
²⁵⁷ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/dd878238\(v=vs.85\).aspx#RD03](http://msdn.microsoft.com/en-us/library/windows/desktop/dd878238(v=vs.85).aspx#RD03)

²⁵⁸ For more information see <http://technet.microsoft.com/en-us/library/dd315291.aspx>

				target output properties. Each property name MUST be unique. If <code>xsi:nil="true"</code> , these pairs are not provided to the cmdlet.
filter	oval-def:filter [2]	0..*	false	Allows for the explicit inclusion or exclusion of <code>cmdlet_items</code> from the set of <code>cmdlet_items</code> collected by a <code>cmdlet_object</code> . Please see the OVAL Language Specification [2] for additional information.

2.75. 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. Certain attributes (such as nouns, verbs, and parameter names) SHOULD align with the MSDN documentation²⁶⁰.



²⁵⁹ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms714395\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms714395(v=vs.85).aspx)

²⁶⁰ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms714423\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms714423(v=vs.85).aspx)

Property	Type	Multiplicity	Nullable	Description
module_name	oval-def:EntityStateStringType	0..1	false	The name of the module that defines the cmdlet 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 .
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 .
module_version	oval-def:EntityStateVersionType	0..1	false	Module version in the format of MAJOR.MINOR ²⁶⁴ .
verb	win-def:EntityStateCmdletVerbType	0..1	false	The verb name of the cmdlet ²⁶⁵ . This verb specifies the action ²⁶⁶ taken by the cmdlet. NOTE: In Windows Powershell, verbs describe a word that <i>implies</i> an action even if that word is not a standard verb in the English language, such as <i>New</i> .
noun	oval-def:EntityStateStringType	0..1	false	The noun name of the cmdlet ²⁶⁷ . This noun specifies the resource ²⁶⁸ that the cmdlet acts upon.
parameters	oval-def:EntityStateRecordType	0..1	false	The parameters of the cmdlet, that is, the list of properties

²⁶¹ For more information see <http://www.microsoft.com/download/en/details.aspx?id=9706>

²⁶² For more information see <http://technet.microsoft.com/en-us/library/dd819471.aspx>

²⁶³ For more information see the examples in <http://technet.microsoft.com/en-us/library/dd819471.aspx>

²⁶⁴ For more information see the examples in <http://technet.microsoft.com/en-us/library/dd819471.aspx>

²⁶⁵ For more information see <http://www.microsoft.com/download/en/details.aspx?id=9706>

²⁶⁶ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms714428\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms714428(v=vs.85).aspx)

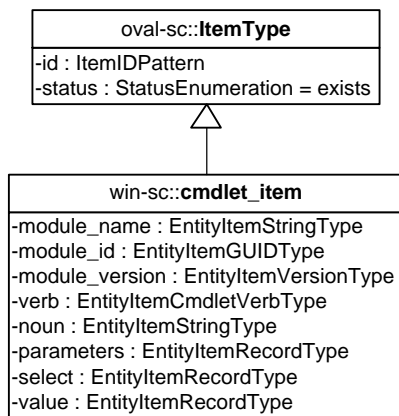
²⁶⁷ For more information see <http://www.microsoft.com/download/en/details.aspx?id=9706>

²⁶⁸ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms714423\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms714423(v=vs.85).aspx)

				(name and value pairs) as input to invoke the cmdlet ²⁶⁹ . Each property name must be unique. Also, parameter names SHOULD align with the MSDN documentation ²⁷⁰ .
select	oval-def: EntityStateRecordType	0..1	false	A set of name and value pairs used as input to the Select-Object 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.

2.76. win-sc:cmdlet_item

The `cmdlet_item` represents a PowerShell cmdlet, the parameters supplied to it, and the value it returned²⁷². Certain attributes (such as nouns, verbs, and parameter names) SHOULD align with the MSDN documentation²⁷³.



²⁶⁹ For more information see <http://www.microsoft.com/download/en/details.aspx?id=9706>

²⁷⁰ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/dd878238\(v=vs.85\).aspx#RD03](http://msdn.microsoft.com/en-us/library/windows/desktop/dd878238(v=vs.85).aspx#RD03)

²⁷¹ For more information see <http://technet.microsoft.com/en-us/library/dd315291.aspx>

²⁷² For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms714395\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms714395(v=vs.85).aspx)

²⁷³ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms714423\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms714423(v=vs.85).aspx)

Property	Type	Multiplicity	Nullable	Description
module_name	oval-sc:EntityItemStringType	0..1	true	<p>The name of the module that defines the cmdlet²⁷⁴. When set using the New-Module command in Powershell, the default name is <code>__DynamicModule_PATHID</code> where "PATHID" is a unique identifier that specifies the path to the dynamic module²⁷⁵.</p> <p>If xsi:nil="true", it implies that it does not matter which module name the command comes from.</p>
module_id	win-sc:EntityItemGUIDType	0..1	true	<p>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 number²⁷⁶.</p> <p>If xsi:nil="true", it implies that it does not matter which module GUID the command comes from.</p>
module_version	oval-sc:EntityItemVersionType	0..1	true	<p>Module version in the format of MAJOR.MINOR²⁷⁷. If xsi:nil="true", it implies that it does not matter which version of the module the command refers to.</p>

²⁷⁴ For more information see <http://www.microsoft.com/download/en/details.aspx?id=9706>

²⁷⁵ For more information see <http://technet.microsoft.com/en-us/library/dd819471.aspx>

²⁷⁶ For more information see the examples in <http://technet.microsoft.com/en-us/library/dd819471.aspx>

²⁷⁷ For more information see the examples in <http://technet.microsoft.com/en-us/library/dd819471.aspx>

verb	win-sc: EntityItemCmdletVerbType	0..1	false	The verb name of the cmdlet ²⁷⁸ . This verb specifies the action ²⁷⁹ taken by the cmdlet. NOTE: In Windows Powershell, verbs describe a word that <i>implies</i> an action even if that word is not a standard verb in the English language, such as <i>New</i> .
noun	oval-sc:EntityItemStringType	0..1	false	The noun name of the cmdlet ²⁸⁰ . This noun specifies the resource 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 . Also, parameter names SHOULD align with the MSDN documentation ²⁸³ .
select	oval-sc:EntityItemRecordType	0..1	true	A set of name and value pairs used as input to the Select-Object 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

²⁷⁸ For more information see <http://www.microsoft.com/download/en/details.aspx?id=9706>

²⁷⁹ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms714428\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms714428(v=vs.85).aspx)

²⁸⁰ For more information see <http://www.microsoft.com/download/en/details.aspx?id=9706>

²⁸¹ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms714423\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms714423(v=vs.85).aspx)

²⁸² For more information see <http://www.microsoft.com/download/en/details.aspx?id=9706>

²⁸³ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/dd878238\(v=vs.85\).aspx#RD03](http://msdn.microsoft.com/en-us/library/windows/desktop/dd878238(v=vs.85).aspx#RD03)

²⁸⁴ For more information see <http://technet.microsoft.com/en-us/library/dd315291.aspx>

				(name and value pairs) that represent the data returned by executing the specified cmdlet on the system. . Each field must have a unique name.
--	--	--	--	------------------------------------------------------------------------------------------------------------------------------------------------

2.77. 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]{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.

2.78. 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]{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.

2.79. 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]{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.

2.80. 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.

2.81. 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.

2.82. 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.

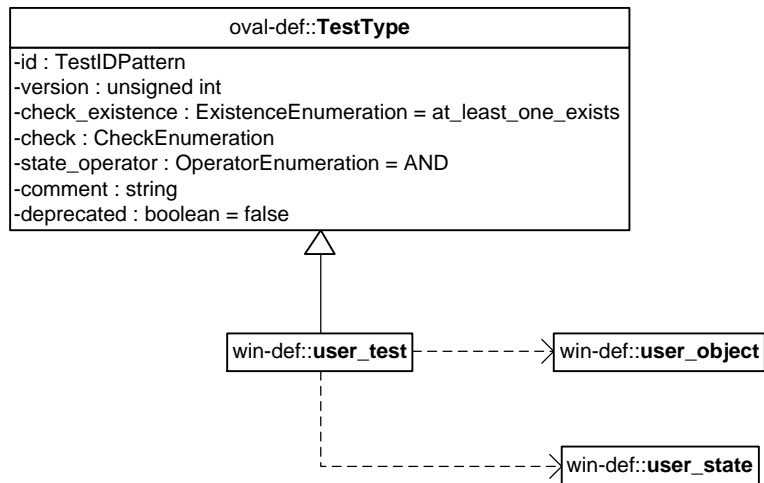
Enumeration Value	Description
Approve	The Approve verb confirms or agrees to the status of a resource or process.
Assert	The Assert verb affirms the state of a resource.
Compare	The Compare verb evaluates the data from one resource against the data from another resource.
Confirm	The Confirm verb acknowledges, 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.

2.83. 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.

²⁸⁵ For more information see <http://technet.microsoft.com/en-us/library/bb726978.aspx>

This test has been deprecated and will be removed in version 6.0 of the language. Due to trustee names not being unique, it is encouraged that you use the `user_sid55_test`.



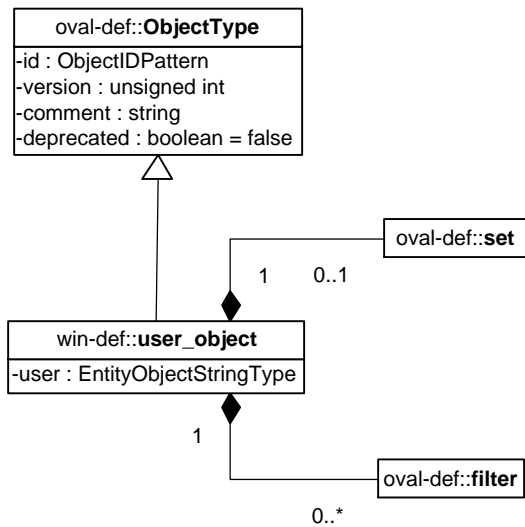
2.83.1. Known Supported Platforms

- Windows XP
- Windows Vista
- Windows 7

2.84. win-def:user_object

The `user_object` construct defines the set of users whose information should be collected and represented as `user_items`.

This object has been deprecated and will be removed in version 6.0 of the language. Due to trustee names not being unique, it is encouraged that you use the `user_sid55_object`.



Property	Type	Multiplicity	Nullable	Description
set	oval-def:set	0..1	false	Enables the expression of complex <code>user_objects</code> that are the result of logically combining and filtering the <code>user_items</code> that are identified by one or more <code>user_objects</code> . 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 . In particular, user account names in

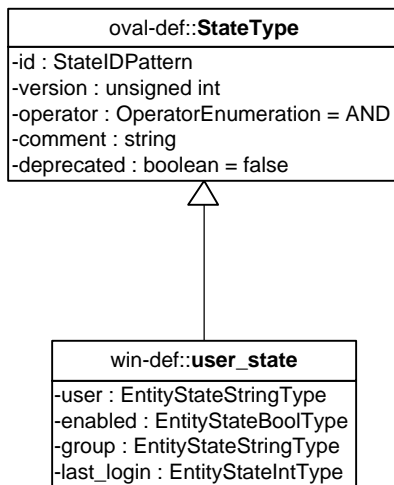
²⁸⁶ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa370653\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa370653(v=vs.85).aspx)

				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 <code>user_items</code> from the set of <code>user_items</code> collected by a <code>user_object</code> . Please see the OVAL Language Specification for additional information.

2.85. 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.

This state has been deprecated and will be removed in version 6.0 of the language. Due to trustee names not being unique, it is encouraged that you use the `user_sid55_state`.



Property	Type	Multiplicity	Nullable	Description
user	oval-def: EntityStateStringType	0..1	false	The user property holds a case-insensitive string that represents the name of a particular user.

				<p>In a domain environment, users SHOULD be identified in the form: "domain\user name". For local users use: "computer name\user name".</p> <p>For built-in accounts on the system, use the user name without a domain. User account names SHOULD align with the MSDN documentation²⁸⁷.</p> <p>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.</p>
enabled	oval-def:EntityStateBoolType	0..1	false	This property holds a boolean value that is <i>true</i> if the particular user account is enabled or <i>false</i> if it is not enabled.
group	oval-def:EntityStateStringType	0..1	false	<p>A case insensitive string that represents the name of a particular group.</p> <p>In a domain environment, groups should be identified in</p>

²⁸⁷ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa370653\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa370653(v=vs.85).aspx)

				<p>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.</p> <p>Group names SHOULD align with the MSDN documentation²⁸⁸.</p> <p>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.</p>
last_logon	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.

2.86. win-sc:user_item

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

This item has been deprecated and will be removed in version 6.0 of the language. Due to trustee names not being unique, it is encouraged that you use the `user_sid_item`.

²⁸⁸ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa370653\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa370653(v=vs.85).aspx)

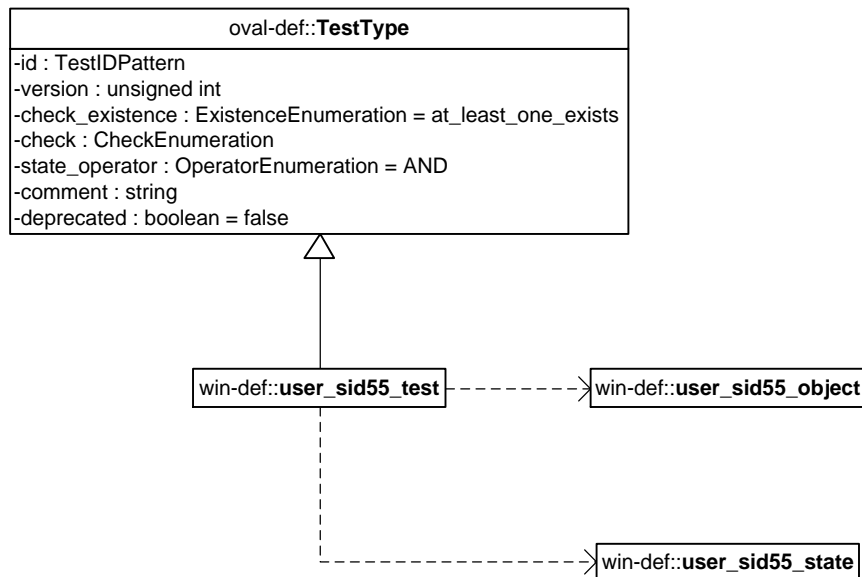
				+ , = , ; , ? , *}, any commas, or non-printable ASCII characters in the range 1-31.
enabled	oval-sc: EntityItemBoolType	0..1	false	This element holds a boolean value that is <i>true</i> if the particular user account is enabled or <i>false</i> if it is not enabled.
group	oval-sc: EntityItemStringType	0..*	false	<p>A string that represents the name of a particular group.</p> <p>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.</p> <p>Group names SHOULD align with the MSDN documentation²⁹⁰. 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.</p>
last_logon	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,

²⁹⁰ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa370653\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa370653(v=vs.85).aspx)

January 1, 1970, GMT.

2.87. 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.



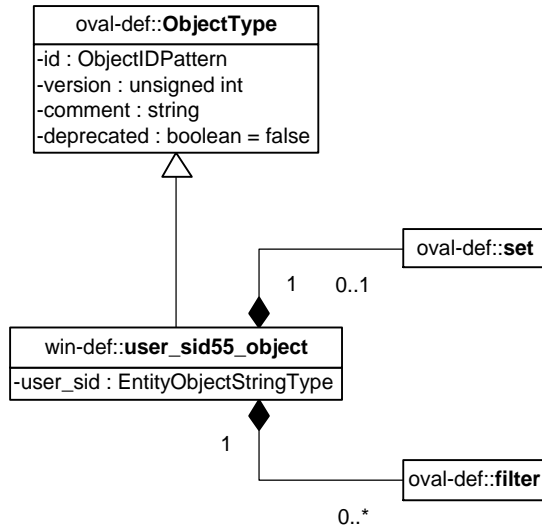
2.87.1. Known Supported Platforms

- Windows XP
- Windows Vista
- Windows 7

²⁹¹ For more information see <http://technet.microsoft.com/en-us/library/bb726978.aspx>

2.88. win-def:user_sid55_object

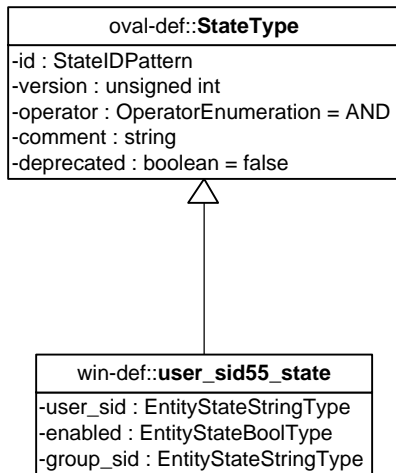
The `user_sid55_object` construct defines the set of users whose information should be collected and represented as `user_sid_items`.



Property	Type	Multiplicity	Nullable	Description
set	oval-def:set	0..1	false	Enables the expression of complex <code>user_sid55_objects</code> that are the result of logically combining and filtering the <code>user_sid_items</code> that are identified by one or more <code>user_sid55_objects</code> . 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 <code>user_items</code> from the set of <code>user_items</code> collected by a <code>user_object</code> . Please see the OVAL Language Specification for additional information.

2.89. win-def:user_sid55_state

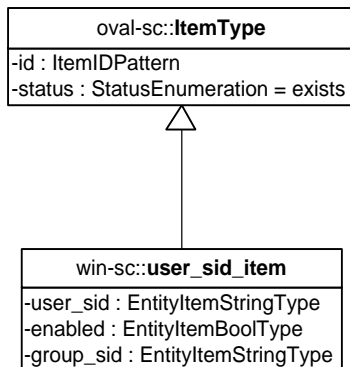
The `user_sid55_state` construct is used by a `user_sid55_test` to specify `user_sid_item` attribute criteria to check on Microsoft Windows platforms.



Property	Type	Multiplicity	Nullable	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 <i>true</i> if the particular user account is enabled or <i>false</i> if it is not enabled.
group_sid	oval-def:EntityStateStringType	0..1	false	A string that represents the SID of a particular group.
last_logon	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.

2.90. win-sc:user_sid_item

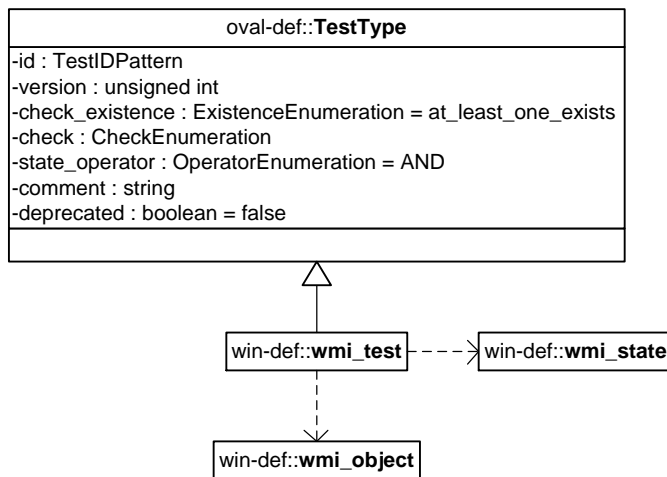
The windows user_sid_item allows the different groups (identified by SID) that a user belongs to, to be collected.



Property	Type	Multiplicity	Nullable	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 <i>true</i> if the particular user account is enabled or <i>false</i> 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.
last_logon	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.

2.91. win-def:wmi_test

The `wmi_test` is used to make assertions about information accessed by WMI²⁹². The `wmi_test` MUST reference one `wmi_object` and zero or more `wmi_states`.



2.91.1. Known Supported Platforms

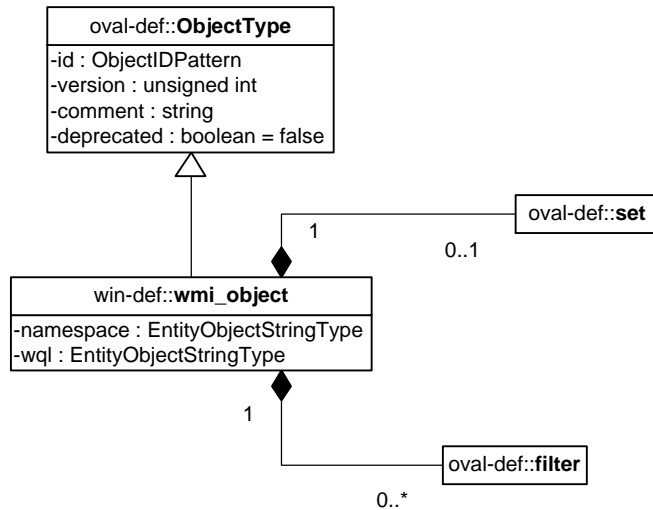
- Windows XP
- Windows Vista
- Windows 7

2.92. win-def:wmi_object

The `wmi_object` construct defines the applicable WMI information that should be collected and represented as `wmi57_items`²⁹³. It allows for single fields to be selected from WMI.

²⁹² For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa394582%28v=vs.85%29.aspx>

²⁹³ For more information see



Property	Type	Multiplicity	Nullable	Description
set	oval-def:set	0..1	false	Enables the expression of complex <code>wmi57_objects</code> that are the result of logically combining and filtering the <code>wmi57_items</code> that are identified by one or more <code>wmi57_objects</code> .
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 .
wql	oval-def:EntityObjectStringType	0..1	false	A WQL query used to identify the <code>wmi_objects</code> to represent as <code>wmi_items</code> . Any valid WQL query is usable with one exception, at most one field is allowed in the SELECT portion of the query ²⁹⁵ .

<http://msdn.microsoft.com/en-us/library/windows/desktop/aa394582%28v=vs.85%29.aspx>

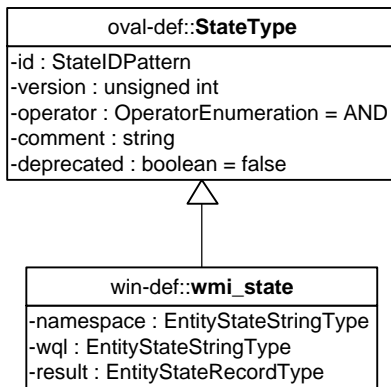
²⁹⁴ For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa394582%28v=vs.85%29.aspx>

²⁹⁵ For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa394606%28v=vs.85%29.aspx>

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.
---------------	---------------------	------	-------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

2.93. 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 platforms²⁹⁶.



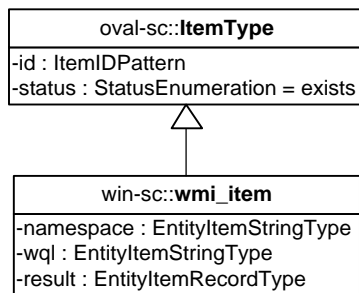
Property	Type	Multiplicity	Nullable	Description
namespace	oval-def: EntityStateStringType	0..1	false	Specifies which WMI namespace to look under. Each WMI provider normally registers its own WMI namespace and then all its

²⁹⁶ For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa394582%28v=vs.85%29.aspx>

				classes within that namespace ²⁹⁷ .
wql	oval-def: EntityStateStringType	0..1	false	A WQL query used to identify the <code>wmi_objects</code> to represent as <code>wmi_items</code> . Any valid WQL query is usable with one exception, at most one field is allowed in the SELECT portion of the query 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.

2.94. win-sc:wmi_item

The `wmi_item` outlines information to be checked through Microsoft's WMI interface.



Property	Type	Multiplicity	Nilable	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

²⁹⁷ For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa394582%28v=vs.85%29.aspx>

²⁹⁸ For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa394606%28v=vs.85%29.aspx>

				classes within that namespace ²⁹⁹ .
wql	oval-sc: EntityItemStringType	0..1	false	A WQL query used to identify the <code>wmi_objects</code> to represent as <code>wmi_items</code> . Any valid WQL query is usable with one exception, at most one field is allowed in the SELECT portion of the query 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.

2.95. win-def:group_test

The `group_test` allows for the testing of different users and subgroups that directly belong to specific groups³⁰¹. A subgroup is an account identified by Name (not by SID) 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 Name into the `LookupAccountName` function³⁰².

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

²⁹⁹ For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa394582%28v=vs.85%29.aspx>

³⁰⁰ For more information see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa394606%28v=vs.85%29.aspx>

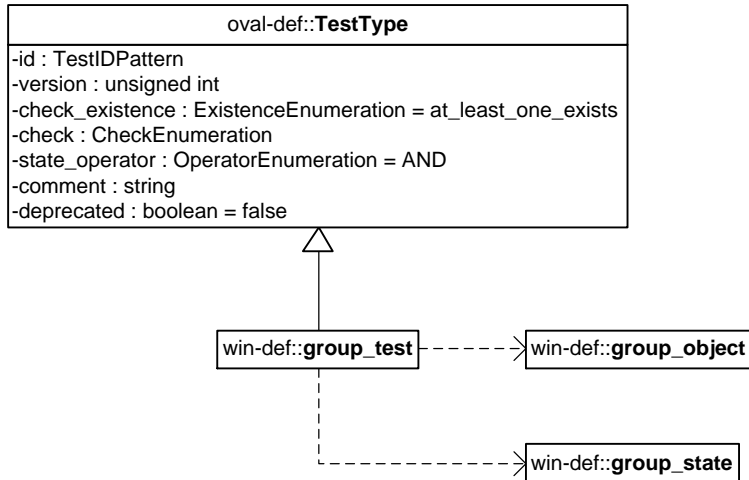
³⁰¹ For more information see [http://technet.microsoft.com/en-us/library/cc739393\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc739393(WS.10).aspx)

³⁰² For more information about `SID_NAME_TYPE` see [http://msdn.microsoft.com/en-us/library/windows/hardware/ff556744\(v=vs.85\).aspx](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](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379166(v=vs.85).aspx)

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`.

This test has been deprecated and will be removed in version 6.0 of the language. Due to trustee names not being unique, it is encouraged that you use the `group_sid_test`.



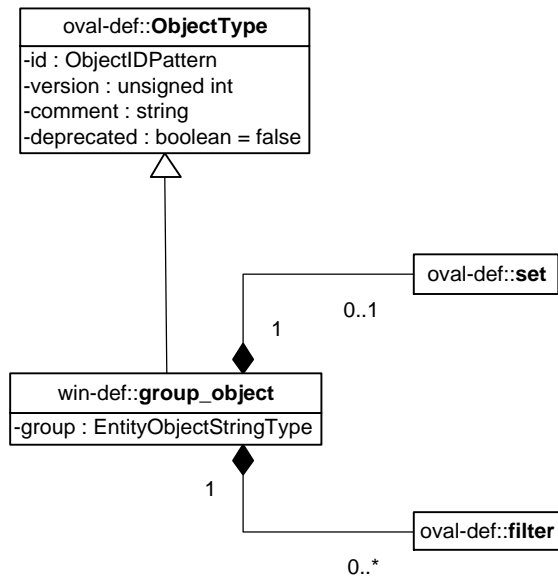
2.95.1. Known Supported Platforms

- Windows XP
- Windows Vista
- Windows 7

2.96. 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`.

This object has been deprecated and will be removed in version 6.0 of the language. Due to trustee names not being unique, it is encouraged that you use the `group_sid_object`.



Property	Type	Multiplicity	Nullable	Description
set	oval-def:set	0..1	false	Enables the expression of complex <code>group_objects</code> that are the result of logically combining and filtering the <code>group_items</code> that are identified by one or more <code>group_objects</code> . Please see the OVAL Language Specification for additional information.
group	oval-def: EntityObjectStringType	1..1	false	<p>A case insensitive string that represents the name of a particular group.</p> <p>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.</p> <p>Group names SHOULD align with the MSDN documentation³⁰³. In particular, group names in Windows are limited to 256 characters and SHOULD NOT contain the following illegal characters in the set {",</p>

³⁰³ For more information see the remarks section of

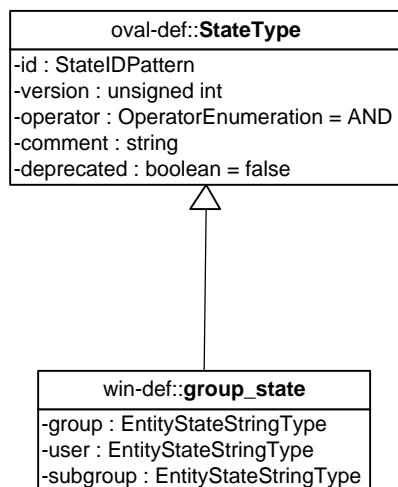
[http://msdn.microsoft.com/en-us/library/windows/desktop/aa370653\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa370653(v=vs.85).aspx)

				/, \, [,], :, , <, >, +, =, ,, ?, *}, 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 <code>group_items</code> from the set of <code>group_items</code> collected by a <code>group_object</code> . Please see the OVAL Language Specification for additional information.

2.97. 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.

This state has been deprecated and will be removed in version 6.0 of the language. Due to trustee names not being unique, it is encouraged that you use the `group_sid_state`.



Property	Type	Multiplicity	Nullable	Description
group	oval-def: EntityStateStringType	0..1	false	A case insensitive string that represents the name of a particular group. In a domain

				<p>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.</p> <p>Group names SHOULD align with the MSDN documentation³⁰⁴. 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.</p>
user	oval-def: EntityStateStringType	0..1	false	<p>A case-insensitive string that represents the name of a particular user.</p> <p>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.</p> <p>User account names</p>

³⁰⁴ For more information see the remarks section of

[http://msdn.microsoft.com/en-us/library/windows/desktop/aa370653\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa370653(v=vs.85).aspx)

				<p>SHOULD align with the MSDN documentation³⁰⁵. 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.</p>
subgroup	oval-def: EntityStateStringType	0..1	false	<p>A case-insensitive string that represents the name of a particular subgroup in the context of the specified group.</p> <p>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.</p> <p>Because a subgroup in Windows is still considered a group, subgroup names SHOULD align with the</p>

³⁰⁵ For more information see the Remarks section of [http://msdn.microsoft.com/en-us/library/windows/desktop/aa370653\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa370653(v=vs.85).aspx)

				<p>MSDN documentation³⁰⁶.</p> <p>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.</p>
--	--	--	--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

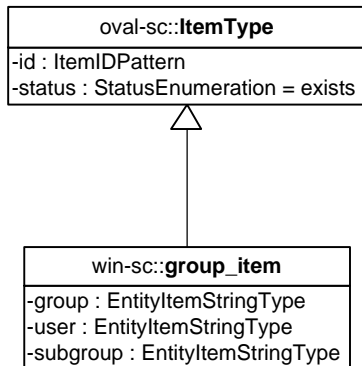
2.98. win-sc:group_item

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'.

This item has been deprecated and will be removed in version 6.0 of the language. Due to trustee names not being unique, it is encouraged that you use the `group_sid_item`.

³⁰⁶ For more information see the Remarks section of [http://msdn.microsoft.com/en-us/library/windows/desktop/aa370653\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa370653(v=vs.85).aspx)



Property	Type	Multiplicity	Nullable	Description
group	oval-sc: EntityItemStringType	0..1	false	<p>A case insensitive string that represents the name of a particular group.</p> <p>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.</p> <p>Group names SHOULD align with the MSDN documentation³⁰⁷. 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</p>

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

				characters in the range 1-31.
user	oval-sc: EntityItemStringType	0..*	false	<p>A case-insensitive string that represents the name of a particular user.</p> <p>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.</p> <p>User account names SHOULD align with the MSDN documentation³⁰⁸. 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.</p>
subgroup	oval-sc: EntityItemStringType	0..*	false	<p>A case-insensitive string that represents the name of a particular subgroup in the context of the specified group.</p> <p>In a domain environment, subgroups should be</p>

³⁰⁸ For more information see the remarks section of

[http://msdn.microsoft.com/en-us/library/windows/desktop/aa370653\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa370653(v=vs.85).aspx)

				<p>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.</p> <p>Because a subgroup in Windows is still considered a group, subgroup names SHOULD align with the MSDN documentation³⁰⁹.</p> <p>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.</p>
--	--	--	--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

2.99. 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` function³¹⁰.

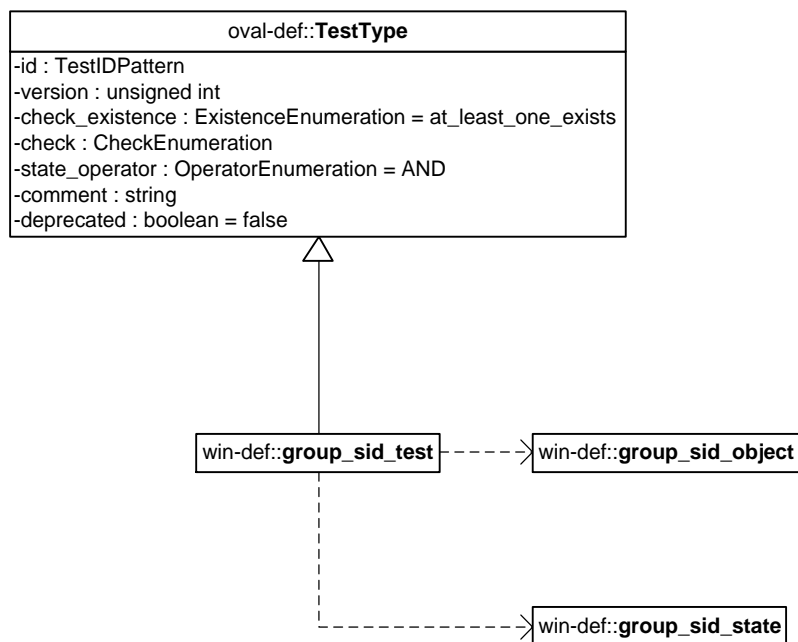
³⁰⁹ For more information see the remarks section of

[http://msdn.microsoft.com/en-us/library/windows/desktop/aa370653\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa370653(v=vs.85).aspx)

³¹⁰ For more information about `SID_NAME_TYPE` see [http://msdn.microsoft.com/en-us/library/windows/hardware/ff556744\(v=vs.85\).aspx](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](http://msdn.microsoft.com/en-us/library/windows/desktop/aa379166(v=vs.85).aspx)

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`.

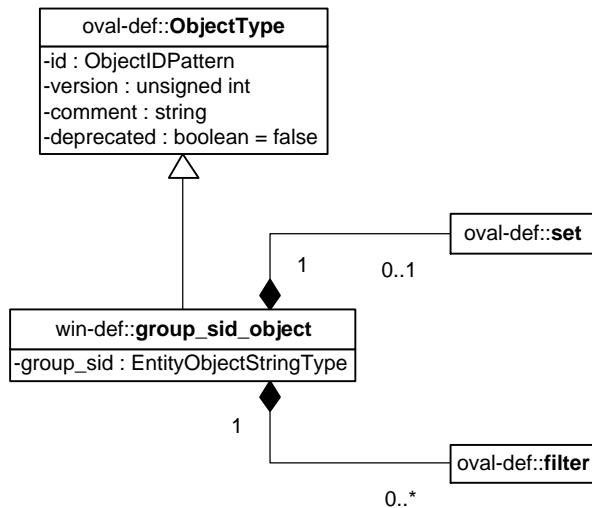


2.99.1. Known Supported Platforms

- Windows XP
- Windows Vista
- Windows 7

2.100. win-def:group_sid_object

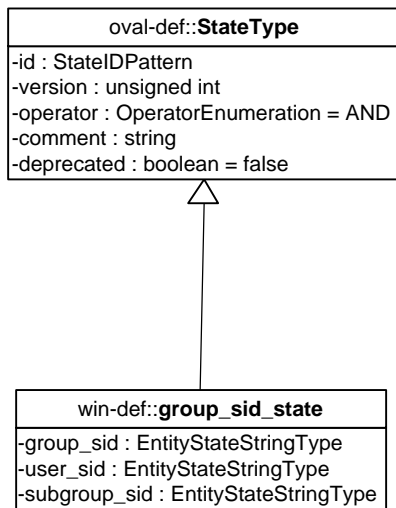
The `group_sid_object` is used by a `group_sid_test` to define the specific group(s) (identified by SID) to be evaluated and represented as `group_sid_items`.



Property	Type	Multiplicity	Nullable	Description
set	oval-def:set	0..1	false	Enables the expression of complex <code>group_sid_objects</code> that are the result of logically combining and filtering the <code>group_sid_items</code> that are identified by one or more <code>group_sid_objects</code> . Please see the OVAL Language Specification for additional information.
group_sid	oval-def:EntityObjectStringType	1..1	false	The <code>group_sid</code> 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 <code>group_sid_items</code> from the set of <code>group_sid_items</code> collected by a <code>group_sid_object</code> . Please see the OVAL Language Specification for additional information.

2.101. win-def:group_sid_state

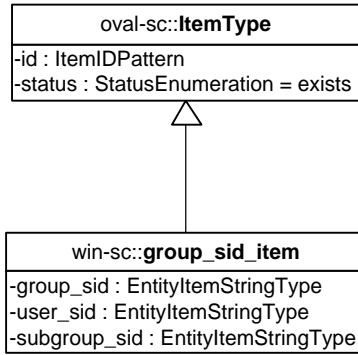
The `group_sid_state` construct is used by a `group_sid_test` to specify `group_sid_item` attribute criteria to check on Microsoft Windows platforms. This test enumerates the different users and subgroups directly associated with a Windows group.



Property	Type	Multiplicity	Nullable	Description
group_sid	oval-def: EntityStateStringType	0..1	false	The <code>group_sid</code> 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 <code>subgroup_sid</code> property holds a string that represents the SID of particular subgroup in the specified group.

2.102. win-sc:group_sid_item

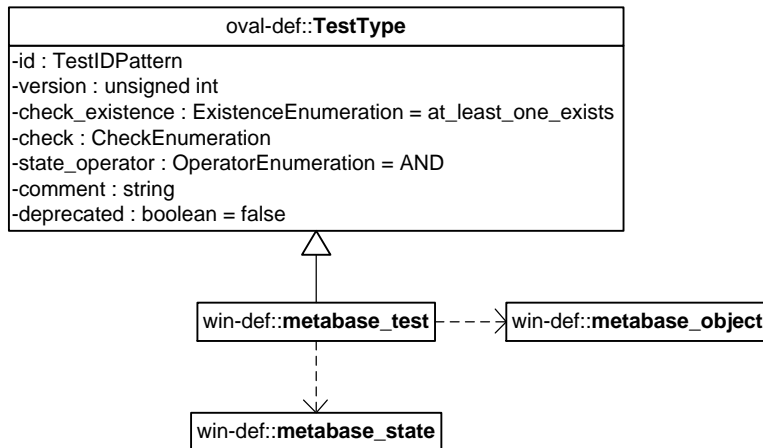
The Windows `group_sid_item` allows the different users and subgroups, that directly belong to specific groups (identified by SID), to be collected. The collected subgroups will not be resolved to find indirect user or subgroup members. If the subgroups need to be resolved, it should be done using the `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	Nullable	Description
group_sid	oval-sc: EntityItemStringType	0..1	false	The <code>group_sid</code> 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 <code>subgroup_sid</code> entity holds a string that represents the SID of particular subgroup in the specified group.

2.103. win-def:metabase_test

The `metabase_test` is used to make assertions about information³¹¹ found in the Windows metabase³¹². The `metabase_test` MUST reference one `metabase_object` and zero or more `metabase_states`.



2.103.1. Known Supported Platforms

- Windows XP
- Windows Vista
- Windows 7

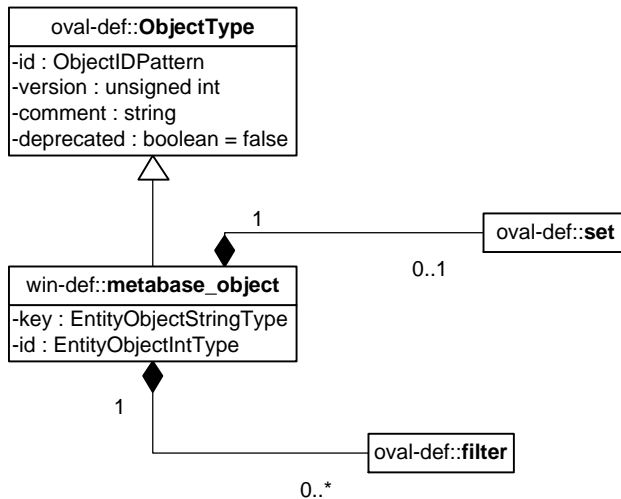
2.104. win-def:metabase_object

The `metabase_object` construct defines the applicable metabase information that should be collected and represented as `metabase_items`³¹³.

³¹¹ For more information see <http://technet.microsoft.com/en-us/query/ms524661>

³¹² For more information see <http://support.microsoft.com/kb/240941>

³¹³ For more information see <http://support.microsoft.com/kb/240941>



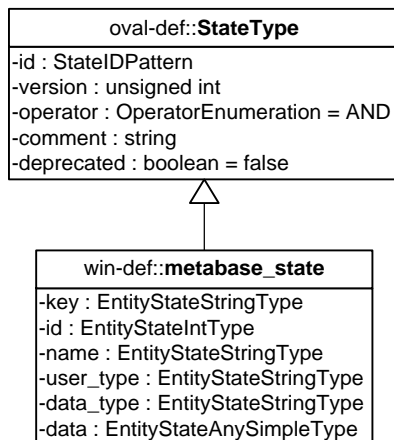
Property	Type	Multiplicity	Nilable	Description
set	oval-def:set	0..1	false	Enables the expression of complex <code>metabase_objects</code> that are the result of logically combining and filtering the <code>metabase_items</code> that are identified by one or more <code>metabase_objects</code> .
key	oval-def:EntityObjectStringType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

³¹⁴ For more information see Metabase Concepts in <http://technet.microsoft.com/en-us/query/ms524661>

³¹⁵ For more information see Internal ID in [http://msdn.microsoft.com/en-us/library/ms524578\(v=vs.90\).aspx#id](http://msdn.microsoft.com/en-us/library/ms524578(v=vs.90).aspx#id)

2.105. 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. The alternate names refer to the variables used in the `METADATA_RECORD`³¹⁷ structure corresponding to specific properties used here.



Property	Type	Multiplicity	Nullable	Description
key	oval-def: EntityStateStringType	0..1	false	This attribute specifies a metabase key ³¹⁸ .
id	oval-def: EntityStateIntType	0..1	false	This attribute specifies a particular object under the metabase key 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: <code>dwMDUserType</code> . This attribute is an integer value that specifies the user type of the data ³²⁰ .
data_type	oval-def: EntityStateStringType	0..1	false	Alternate name: <code>dwMDDataType</code> . The <code>data_type</code> element identifies

³¹⁶ For more information see [http://msdn.microsoft.com/en-us/library/cc233554\(v=PROT.10\).aspx](http://msdn.microsoft.com/en-us/library/cc233554(v=PROT.10).aspx)

³¹⁷ For more information see [http://msdn.microsoft.com/en-us/library/cc233554\(v=PROT.10\).aspx](http://msdn.microsoft.com/en-us/library/cc233554(v=PROT.10).aspx)

³¹⁸ For more information see Metabase Concepts in <http://technet.microsoft.com/en-us/query/ms524661>

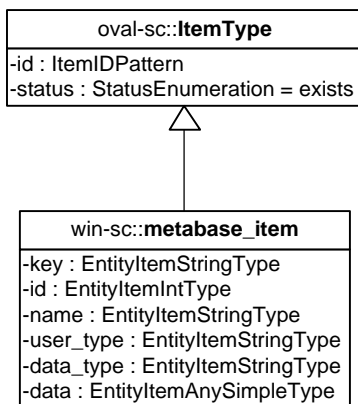
³¹⁹ For more information see Internal ID in [http://msdn.microsoft.com/en-us/library/ms524578\(v=vs.90\).aspx#id](http://msdn.microsoft.com/en-us/library/ms524578(v=vs.90).aspx#id)

³²⁰ For more information see [http://msdn.microsoft.com/en-us/library/ms524635\(v=VS.90\).aspx](http://msdn.microsoft.com/en-us/library/ms524635(v=VS.90).aspx)

				the type of data in the metabase entry ³²¹ .
data	oval-def: EntityStateAnySimpleType	0..1	false	Alternate name: The actual data of the named item under the specified metabase key ³²² . This includes property attributes, usertype, datatype number of data entries, and others that can be obtained via the GetAllData method ³²³ .

2.106. win-sc:metabase_item

The `metabase_item` gathers information from the specified metabase keys³²⁴.



Property	Type	Multiplicity	Nilable	Description
key	oval-sc: EntityItemStringType	0..1	false	This attribute specifies a metabase key ³²⁵ .
id	oval-sc:EntityItemIntType	0..1	true	This attribute specifies a particular object under the metabase key ³²⁶ .
name	oval-sc: EntityItemStringType	0..1	false	This attribute describes the name of the specified

³²¹ For more information see [http://msdn.microsoft.com/en-us/library/ms524635\(v=VS.90\).aspx](http://msdn.microsoft.com/en-us/library/ms524635(v=VS.90).aspx)

³²² For more information see Property Attributes in [http://msdn.microsoft.com/en-us/library/ms524578\(v=vs.90\).aspx](http://msdn.microsoft.com/en-us/library/ms524578(v=vs.90).aspx)

³²³ For more information see [http://msdn.microsoft.com/en-us/library/ms524951\(v=vs.90\).aspx](http://msdn.microsoft.com/en-us/library/ms524951(v=vs.90).aspx)

³²⁴ For more information see [http://msdn.microsoft.com/en-us/library/cc233554\(v=PROT.10\).aspx](http://msdn.microsoft.com/en-us/library/cc233554(v=PROT.10).aspx)

³²⁵ For more information see Metabase Concepts in <http://technet.microsoft.com/en-us/query/ms524661>

³²⁶ For more information see Internal ID in [http://msdn.microsoft.com/en-us/library/ms524578\(v=vs.90\).aspx#id](http://msdn.microsoft.com/en-us/library/ms524578(v=vs.90).aspx#id)

				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 .
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 .
data	oval-sc: EntityItemAnySimpleType	0..*	false	Alternate name: The actual data of the named item under the specified metabase key ³²⁹ . This includes property attributes, usertype, datatype number of data entries, and others that can be obtained via the GetAllData method ³³⁰ .

³²⁷ For more information see [http://msdn.microsoft.com/en-us/library/ms524635\(v=VS.90\).aspx](http://msdn.microsoft.com/en-us/library/ms524635(v=VS.90).aspx)

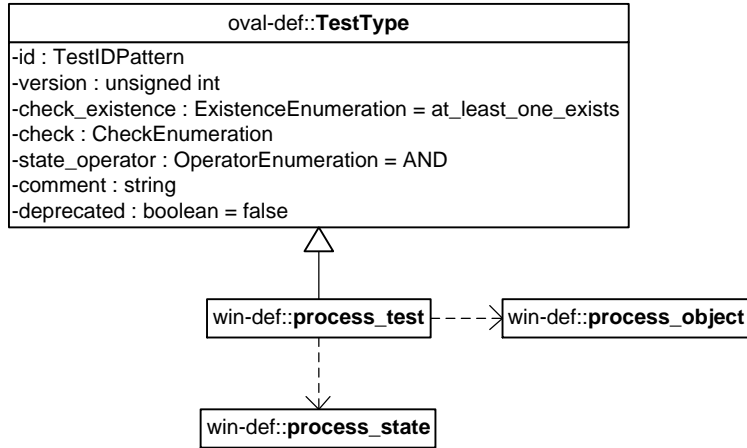
³²⁸ For more information see [http://msdn.microsoft.com/en-us/library/ms524635\(v=VS.90\).aspx](http://msdn.microsoft.com/en-us/library/ms524635(v=VS.90).aspx)

³²⁹ For more information see Property Attributes in [http://msdn.microsoft.com/en-us/library/ms524578\(v=vs.90\).aspx](http://msdn.microsoft.com/en-us/library/ms524578(v=vs.90).aspx)

³³⁰ For more information see [http://msdn.microsoft.com/en-us/library/ms524951\(v=vs.90\).aspx](http://msdn.microsoft.com/en-us/library/ms524951(v=vs.90).aspx)

2.107. win-def:process_test

The `process_test` is used to make assertions about information found in Windows processes³³¹.
 The `process_test` MUST reference one `process_object` and zero or more `process_states`.

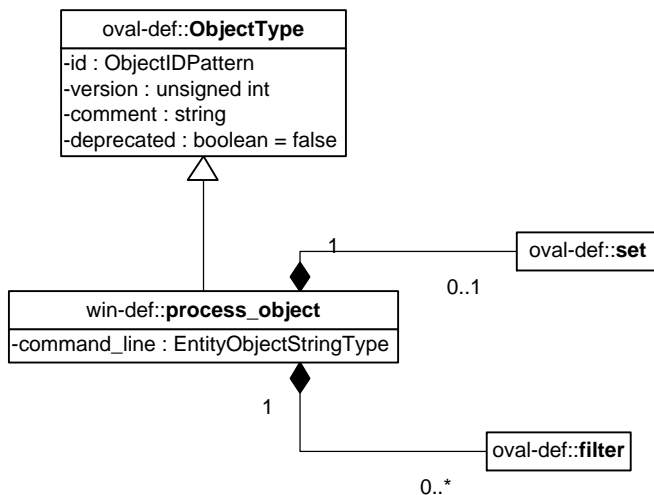


2.107.1. Known Supported Platforms

- Windows XP
- Windows Vista
- Windows 7

2.108. 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	Nullable	Description
----------	------	--------------	----------	-------------

³³¹ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms681917\(v=VS.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms681917(v=VS.85).aspx)

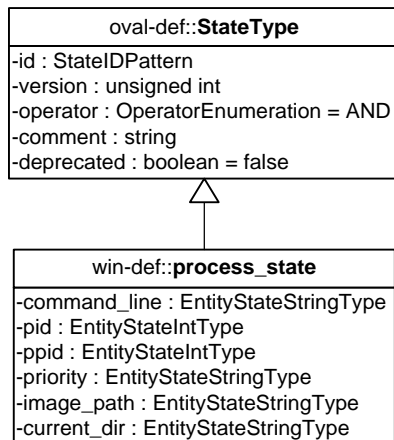
set	oval-def:set	0..1	false	Enables the expression of complex <code>process_objects</code> that are the result of logically combining and filtering the <code>process_items</code> that are identified by one or more <code>process_objects</code> .
command_line	oval-def: EntityObjectStringType	0..1	false	The string used to start the process 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 <code>process_items</code> from the set of <code>process_items</code> collected by a <code>process_object</code> . Please see the OVAL Language Specification [2] for additional information.

2.109. `win-def:process_state`

The `process_state` construct is used by a `process_test` to outline information about Windows processes³³³. 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.

³³² For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa394372\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa394372(v=vs.85).aspx)

³³³ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms681917\(v=VS.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms681917(v=VS.85).aspx)



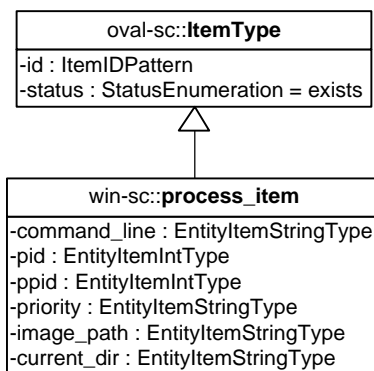
Property	Type	Multiplicity	Nullable	Description
command_line	oval-def: EntityStateStringType	0..1	false	Alternate name: Command Line. The string used to start the process ³³⁴ . This includes any parameters that are part of the command line.
pid	oval-def:EntityStateIntType	0..1	false	Alternate name: PID. 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 executable name itself. In other words, if y.exe was found in path x:\, then

³³⁴ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa394372\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa394372(v=vs.85).aspx)

				image_path would return y.exe and current_dir would return x:\. Image Path Name returns x:\y.exe in Task Manager.
--	--	--	--	-------------------------------------------------------------------------------------------------------------------

2.110. win-sc:process_item

The `process_item` gathers information from the specified Windows processes³³⁵. 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	Nilable	Description
command_line	oval-sc: EntityItemStringType	0..1	false	Alternate name: Command Line. The string used to start the process 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:	0..1	false	Alternate name: Image

³³⁵ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/ms681917\(v=VS.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms681917(v=VS.85).aspx)

³³⁶ For more information see [http://msdn.microsoft.com/en-us/library/windows/desktop/aa394372\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa394372(v=vs.85).aspx)

	EntityItemStringType			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 executable 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 5 – December 18, 2014

- Updated version and date information for the Official 5.11 Release.

Version 5.11 Revision 4 – December 01, 2014

- Updated version and date information for 5.11 Release Candidate 2.

Version 5.11 Revision 3 – November 18, 2014

- Updated version and date information for 5.11 Release Candidate 1.
- Added deprecation messages to the accesstoken_test, user_test, group_test, and their related objects, states, items, and behaviors.

Version 5.11 Revision 2 – September 25, 2013

- Added last_logon entity to user_sid55_state and user_sid_item. (Section 2.89, 2.90)
- Corrected spelling errors on last_logon entities for user_state and user_item elements. (Section 2.86)
- Added a sentence to the win-def:group_test documentation that defines the subgroup display type and clarifies the API used to obtain it. This addresses <https://github.com/OVALProject/Language/issues/132>. (Section 2.95)
- Added new reg type entries into:
 - win-def:entityStateRegistryTypeType description table (Section 2.22)
 - win-sc:EntityItemRegistryTypeType description table (Section 2.23)
 - <https://github.com/OVALProject/Language/issues/102>

Version 5.11 Revision 1 – February 20, 2013

- Removed the restriction that required the name entity in the win-def:registry_test to be nilled when the key entity was nilled. This addresses <https://github.com/OVALProject/Language/issues/1>.
- 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