THE MITRE CORPORATION

The OVAL® Language Windows Component Model Specification

Version 5.10.1

Danny Haynes, Stelios Melachrinoudis

1/19/2012

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

Acknowledgements

Trademark Information

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

Warnings

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

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.org[2].

[1] For more information see https://oval.mitre.org/about/termsofuse.html

[2] For more information see https://oval.mitre.org/

Contents

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

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

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

1.2 Document Structure

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

[3] For more information see 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

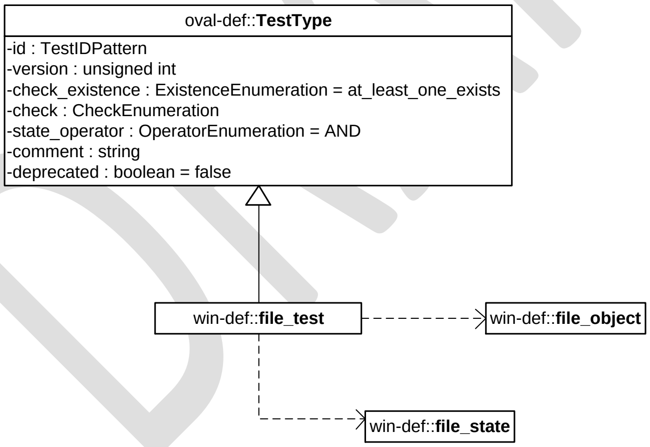
The OVAL Language Windows Component Data Model is the platform-specific extension of the OVAL Language Data Model for Microsoft Windows operating systems.

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 files[4] on file systems supported by Microsoft Windows operating systems. The `file_test` MUST reference one `file_object` and zero or more `file_states`.


oval-def::TestType
-id : TestIDPattern
-version : unsigned int
-check_existence : ExistenceEnumeration = at_least_one_exists
-check : CheckEnumeration
-state_operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::file_test
win-def::file_object
win-def::file_state

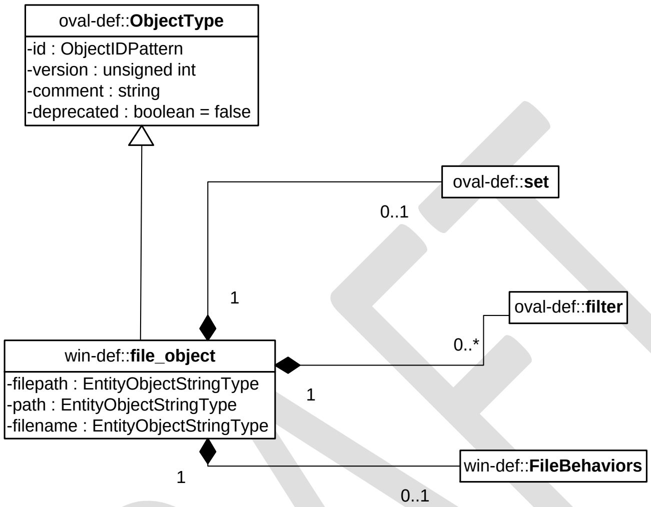
2.2.1 Known Supported Platforms

- Windows XP
- Windows Vista
- Windows 7

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

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	Nillable	Description
set	oval-def:set	0..1	false	Enables the expression of complex `file_objects` that are the result of logically combining and filtering the `file_items` that are identified by one or more `file_objects`. The behaviors, filepath, path, filename, and filter properties MUST NOT be specified when this property is specified . Please see the OVAL Language Specification for additional information.
behaviors	win-def:FileBehaviors	0..1	false	Specifies the behaviors that direct how the `file_object` collects `file_items` from the system.
filepath	oval-def:	0..1	false	The absolute path to a file on the system.

	EntityObjectStringType			The absolute path SHOULD align with the guidance provided in the MSDN documentation[5]. A directory MUST NOT be specified for this property. The path and filename properties MUST NOT be specified when this property is specified. The max_depth and recurse_direction behaviors MUST NOT be used in conjunction with this property as they are reserved for use with the path and filename properties.
path	oval-def: EntityObjectStringType	0..1	false	The directory component of the absolute path to a directory or file on the system. The path component SHOULD align with the guidance provided in the MSDN documentation[6]. The filepath property MUST NOT be specified when this property is specified.
filename	oval-def: EntityObjectStringType	0..1	true	The name of a file to evaluate. A filename MUST NOT contain the characters in the set { /, \, ?, |, >, :, *}. The filename SHOULD also align with the guidance provided in the MSDN documentation, as there are more conventions when naming files beyond the characters listed above[7]. The filepath property MUST NOT be specified when this property is specified. **xsi:nil="true"** indicates that the `file_object` MUST collect the set of directories specified by the path entity. In addition, a value for the filename entity

[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 `file_items` from the set of `file_items` collected by a `file_object`. 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.

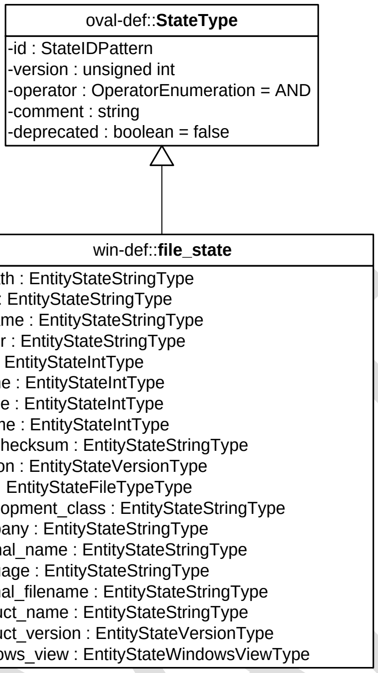
Attribute	Type	Possible Values	Description
max_depth	integer	< *-1* *-1* *0* > *0*	Defines the maximum depth of file system traversal when the recurse_direction behavior is set to a value other than *'none'*. < *-1*: not permitted. *-1***:** traverse the file system with no limitation. *0***:** do not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

			An error MUST NOT be reported when the max_depth behavior specifies a certain level of traversal and that level does not exist. **Default Value: none**
recurse_file_system	string	*'all'* *'local'* *'defined'*	Defines the file system limitation of any searching. This applies to all operations as specified in the path or filepath entity. *'all'*: traverse both local and remote file systems. *'local'*: only traverse the local file systems. *'defined'*: only traverse the specified file system. The value of *'defined'* MUST only be used in conjunction with the equality operation because the path or filepath entity must explicitly define a file system. **Default Value: all**
windows_view	string	*'32_bit'* *'64_bit'*	64-bit versions of Windows provide an alternate file system view to 32-bit applications[8]. This behavior defines which view should be examined by the `file_object`. *'32_bit'*: check the 32_bit view of the file system. *'64_bit'*: check the 64_bit view of the file system. This behavior only applies to 64-bit versions of Windows and MUST NOT be applied on other platforms. **Default Value: 64-bit**

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


oval-def::StateType
-id : StateIDPattern
-version : unsigned int
-operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::file_state
-filepath : EntityStateStringType
-path : EntityStateStringType
-filename : EntityStateStringType
-owner : EntityStateStringType
-size : EntityStateIntType
-a_time : EntityStateIntType
-c_time : EntityStateIntType
-m_time : EntityStateIntType
-ms_checksum : EntityStateStringType
-version : EntityStateVersionType
-type : EntityStateFileTypeType
-development_class : EntityStateStringType
-company : EntityStateStringType
-internal_name : EntityStateStringType
-language : EntityStateStringType
-original_filename : EntityStateStringType
-product_name : EntityStateStringType
-product_version : EntityStateVersionType
-windows_view : EntityStateWindowsViewType

Property	Type	Multiplicity	Nillable	Description
filepath	oval-def:EntityStateStringType	0..1	false	The absolute path to a file on the system. The absolute path SHOULD align with the guidance provided in the MSDN documentation[9]. A directory MUST NOT be specified for this property. The max_depth and recurse_direction behaviors MUST NOT be used in conjunction with this property as

[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	The directory component of the absolute path to a directory or file on the system. The path component SHOULD align with the guidance provided in the MSDN documentation[10].
filename	oval-def:EntityStateStringType	0..1	false	The name of a file to evaluate. A filename MUST NOT contain the characters in the set { /, \, ?, |, >, :, *}. The filename SHOULD also align with the guidance provided in the MSDN documentation, as there are more conventions when naming files beyond the characters listed above[11].
owner	oval-def:EntityStateStringType	0..1	false	The owner of the file. The owner MUST BE expressed in the DOMAIN\username format. The username component of the owner can be retrieved using the GetSecurityInfo function[12] and the

[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

				domain component can be retrieved using the LookupAccountSid function[13].
Size	oval-def:EntityStateIntType	0..1	false	The size of the file in bytes. The size of the file can be retrieved using the _stat function[14] or GetFileSizeEx function[15].
a_time	oval-def:EntityStateIntType	0..1	false	The date and time that the file was last accessed. This is valid on NTFS formatted disk drives, but, not on FAT formatted disk drives. This value MUST align with the FILETIME structure which contains a 64-bit number representing how many 100-nanosecond intervals have passed since January 1, 1601 (UTC)[16]. The GetFileTime function[17] can retrieve the last accessed time.
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

[14] For more information see 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

[16] For more information see 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

				This is valid on NTFS formatted disk drives, but, not on FAT formatted disk drives. This value MUST align with the FILETIME structure which contains a 64-bit number representing how many 100-nanosecond intervals have passed since January 1, 1601 (UTC)[18]. The GetFileTime function[19] can retrieve the creation time.
m_time	oval-def:EntityStateIntType	0..1	false	The date and time that the file was last modified. This value MUST align with the FILETIME structure which contains a 64-bit number representing how many 100-nanosecond intervals have passed since January 1, 1601 (UTC)[20]. The GetFileTime function[21] can retrieve the last modified time.
ms_checksum	oval-def:EntityStateStringType	0..1	false	The checksum of the file. The checksum MUST

[18] For more information see 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

[20] For more information see 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

				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 mmmmmm-nnnn

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

				component of the file version formats[27]. This value can be obtained via the VarQueryValue function[28].
company	oval-def:EntityStateStringType	0..1	false	The name of the company that created the file. This value can be obtained via the VarQueryValue function[29] or the FileVersionInfo class[30].
internal_name	oval-def:EntityStateStringType	0..1	false	The internal name of the file. This value can be obtained via the VarQueryValue function[31] or the FileVersionInfo class[32].
language	oval-def:EntityStateStringType	0..1	false	The description string for the Microsoft Language Identifier associated with the file. This value can be obtained via the VarQueryValue function[33] or the FileVersionInfo class[34].
original_filename	oval-def:EntityStateStringType	0..1	false	The original name of the file when it was created.

[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
[29] For more information see 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
[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
[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.

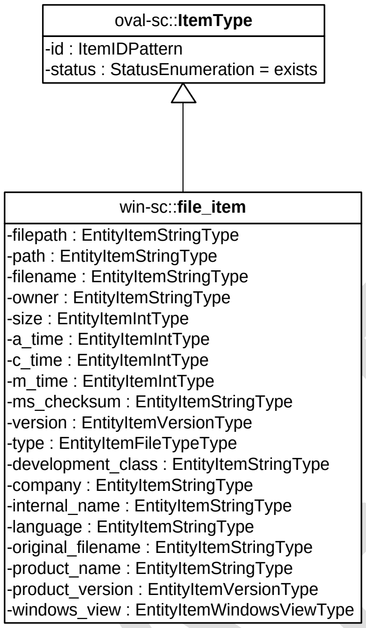
2.6 win-sc:file_item

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
[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
[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
[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


oval-sc::ItemType
-id : ItemIDPattern
-status : StatusEnumeration = exists
win-sc::file_item
-filepath : EntityItemStringType
-path : EntityItemStringType
-filename : EntityItemStringType
-owner : EntityItemStringType
-size : EntityItemIntType
-a_time : EntityItemIntType
-c_time : EntityItemIntType
-m_time : EntityItemIntType
-ms_checksum : EntityItemStringType
-version : EntityItemVersionType
-type : EntityItemFileTypeType
-development_class : EntityItemStringType
-company : EntityItemStringType
-internal_name : EntityItemStringType
-language : EntityItemStringType
-original_filename : EntityItemStringType
-product_name : EntityItemStringType
-product_version : EntityItemVersionType
-windows_view : EntityItemWindowsViewType

Property	Type	Multiplicity	Nillable	Description
filepath	oval-sc: EntityItemStringType	0..1	false	The absolute path to a file on the system. The absolute path SHOULD align with the guidance provided in the MSDN documentation[42]. A directory MUST NOT be specified for this property. The max_depth and recurse_direction behaviors MUST NOT be used in conjunction with this property as they are reserved for use with the path and filename properties.

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

path	oval-sc: EntityItemStringType	0..1	false	The directory component of the absolute path to a directory or file on the system. The path component SHOULD align with the guidance provided in the MSDN documentation[43].
filename	oval-sc: EntityItemStringType	0..1	true	The name of a file to evaluate. A filename MUST NOT contain the characters in the set { /, \, ?, |, >, :, *}. The filename SHOULD also align with the guidance provided in the MSDN documentation, as there are more conventions when naming files beyond the characters listed above[44]. **xsi:nil="true"** MUST be set when the filename entity, in the collecting `file_object`, has xsi:nil="true" set. In addition, the status of this entity MUST be *'not collected'* and a value for this entity MUST NOT be specified.
owner	oval-sc: EntityItemStringType	0..1	false	The owner of the file. The owner MUST BE expressed in the

[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

				DOMAIN\username format. The username component of the owner can be retrieved using the GetSecurityInfo function[45] and the domain component can be retrieved using the LookupAccountSid function[46].
size	oval-sc:EntityItemIntType	0..1	false	The size of the file in bytes. The size of the file can be retrieved using the _stat function[47] or GetFileSizeEx function[48].
a_time	oval-sc:EntityItemIntType	0..1	false	The date and time that the file was last accessed. This is valid on NTFS formatted disk drives, but, not on FAT formatted disk drives. This value MUST align with the FILETIME structure which contains a 64-bit number representing how many 100-nanosecond intervals have passed since January 1, 1601 (UTC)[49].

[45] For more information see 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
[47] For more information see 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
[49] For more information see 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	The date and time that the file was created. This is valid on NTFS formatted disk drives, but, not on FAT formatted disk drives. This value MUST align with the FILETIME structure which contains a 64-bit number representing how many 100-nanosecond intervals have passed since January 1, 1601 (UTC)[51]. The GetFileTime function[52] can retrieve the creation time.
m_time	oval-sc:EntityItemIntType	0..1	false	The date and time that the file was last modified. This value MUST align with the FILETIME structure which contains a 64-bit number representing how many 100-nanosecond intervals have passed since January 1, 1601 (UTC)[53].

[50] For more information see 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
[52] For more information see 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

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

				releases (GDR) development environment and the quick fix engineering (QFE) development environment. This value MUST be the text prior to the mmmmmm-nnnn component of the file version formats[60]. This value can be obtained via the VarQueryValue function[61].
company	oval-sc: EntityItemStringType	0..1	false	The name of the company that created the file. This value can be obtained via the VarQueryValue function[62] or the FileVersionInfo class[63].
internal_name	oval-sc: EntityItemStringType	0..1	false	The internal name of the file. This value can be obtained via the VarQueryValue function[64] or the FileVersionInfo class[65].
language	oval-sc: EntityItemStringType	0..1	false	The description string for the Microsoft Language Identifier associated with the file.

[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
[62] For more information see 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
[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
[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

[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
[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
[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

				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
FILE_ATTRIBUTE_ DIRECTORY	This value indicates a directory.
FILE_TYPE_CHAR	This value indicates a character file, typically an LPT device or a console.
FILE_TYPE_DISK	This value indicates a disk file.
FILE_TYPE_PIPE	This value indicates a socket, a named pipe, or an anonymous pipe.
FILE_TYPE_REMOTE	This value is currently unused by Microsoft.
FILE_TYPE_UNKNOWN	This value indicates that the type of file is unknown.
<empty string>	This value indicates that no value has been specified and is permitted here to allow for an empty entity which is associated with a reference to an OVAL Variable.

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
FILE_ATTRIBUTE_DIRECTORY	This value indicates a directory.
FILE_TYPE_CHAR	This value indicates a character file, typically an LPT device or a console.
FILE_TYPE_DISK	This value indicates a disk file.
FILE_TYPE_PIPE	This value indicates a socket, a named pipe, or an anonymous pipe.
FILE_TYPE_REMOTE	This value is currently unused by Microsoft.
FILE_TYPE_UNKNOWN	This value indicates that the type of file is unknown.
<empty string>	This value indicates that no value has been specified and is permitted here to allow for an empty entity which is associated with error and not collected conditions.

2.12. win-def:EntityStateWindowsViewType

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

Enumeration Value	Description
32_bit	This value indicates the 32-bit view.
64_bit	This value indicates the 64-bit view.

<empty string>	This value indicates that no value has been specified and is permitted here to allow for an empty entity which is associated with a reference to an OVAL Variable.

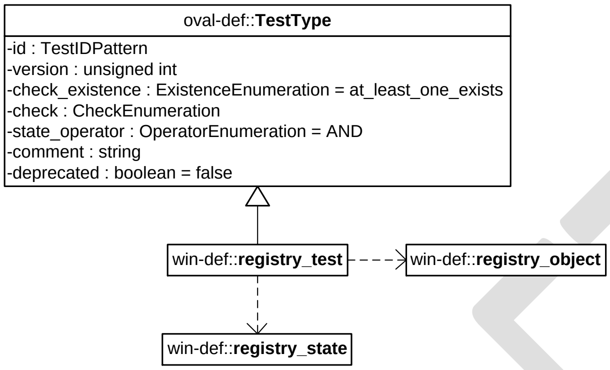
2.13. win-sc:EntityItemWindowsViewType

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 registry[75] on Microsoft Windows operating systems. The registry_test MUST reference one registry_object and zero or more registry_states.


oval-def::TestType
-id : TestIDPattern
-version : unsigned int
-check_existence : ExistenceEnumeration = at_least_one_exists
-check : CheckEnumeration
-state_operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::registry_test
win-def::registry_object
win-def::registry_state

2.14.1. Known Supported Platforms

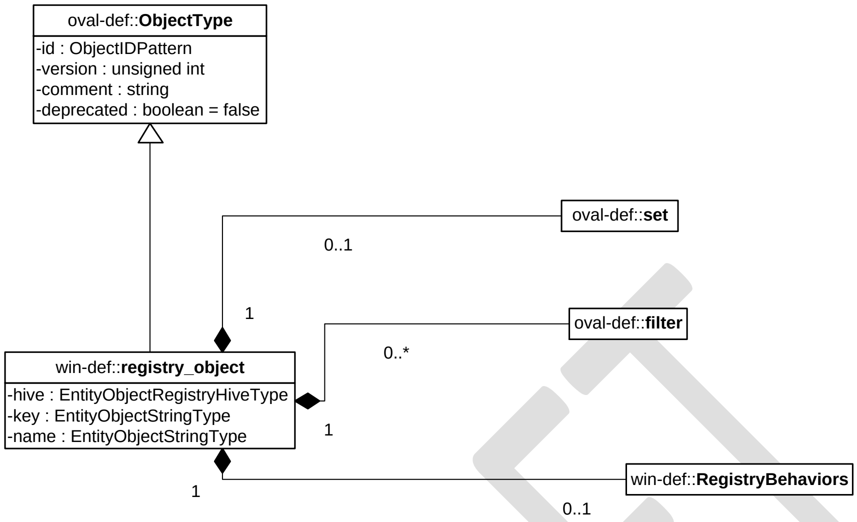
- Windows XP
- Windows Vista
- Windows 7

Comment [DJH1]: We probably want to consider adding windows 2000, windows server 2003, windows server 2008, and windows server 2008 r2.

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


oval-def::ObjectType
-id : ObjectIDPattern
-version : unsigned int
-comment : string
-deprecated : boolean = false
oval-def::set
0..1
1
oval-def::filter
0..*
win-def::registry_object
-hive : EntityObjectRegistryHiveType
-key : EntityObjectStringType
-name : EntityObjectStringType
1
win-def::RegistryBehaviors
1
0..1

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

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

[76] For more information see 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.

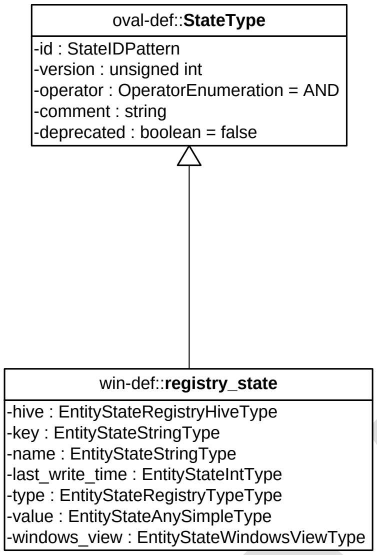
Attribute	Type	Possible Values	Description
max_depth	integer	*< -1* *-1* *0* *> 0*	Defines the maximum depth of registry traversal when the recurse_direction behavior is set to a value other than *'none'*. < *-1*: not permitted. *-1***:** traverse the registry with no limitation. *0***:** do not traverse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

			'down': traverse the registry by recursively visiting the child keys. Note: It is not an error if max_depth specifies a certain level of traversal and that level does not exist. **Default Value: none**
windows_view	string	*'32_bit'* *'64_bit'*	64-bit versions of Windows provide an alternate registry view to 32-bit applications[77]. This behavior defines which view should be examined by the `registry_object`. *'32_bit'*: check the 32_bit view of the registry. *'64_bit'*: check the 64_bit view of the registry. This behavior only applies to 64-bit versions of Windows and MUST NOT be applied on other platforms. **Default Value: 64-bit**

[77] For more information see 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.


oval-def::StateType
-id : StateIDPattern
-version : unsigned int
-operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::registry_state
-hive : EntityStateRegistryHiveType
-key : EntityStateStringType
-name : EntityStateStringType
-last_write_time : EntityStateIntType
-type : EntityStateRegistryTypeType
-value : EntityStateAnySimpleType
-windows_view : EntityStateWindowsViewType

Property	Type	Multiplicity	Nillable	Description
hive	win-def: EntityStateRegistryHiveType	0..1	false	The hive that the registry key belongs to. This SHOULD align with the guidance provided in the MSDN documentation, which contains the list of predefined hives[78].
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.

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

				If an empty string is specified, the registry key's default value MUST be collected. This can be obtained using the RegQueryValueEx function[79].
last_write_time	oval-def:EntityStateIntType	0..1	false	The date and time that the key or any of its value entries were last modified. This value MUST align with the FILETIME structure which contains a 64-bit number representing how many 100-nanosecond intervals have passed since January 1, 1601 (UTC)[80]. The last write time can be queried on a hive, key, or name. When collecting only information about a registry hive the last write time will be the time the hive or any of its entiries was written to. When collecting only information about a registry hive and key the last write time will be the time the key or any of its entiries was written to. When collecting only

[79] For more information see 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

				information about a registry name the last write time will be the time the name was written to. This can be obtained using the RegQueryInfoKey function[81].
type	win-def: EntityStateRegistryTypeType	0..1	false	The type associated with the value of a hive or registry key. This can be obtained using the RegQueryValueEx function[82].
value	oval-def: EntityStateAnySimpleType	0..*	false	The value(s) associated with a hive or registry key. The value of a hive or registry key can be obtained using the RegQueryValueEx function[83]. Please see the OVAL Language Specification [2] for more information about how datatypes are assigned to OVAL Item Entities.
windows_view	win-def: EntityStateWindowsViewType	0..1	false	The targeted registry view[84] where the hive or registry key was collected.

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

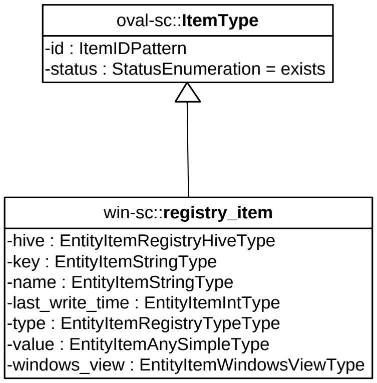
[82] For more information see http://msdn.microsoft.com/en-us/library/windows/desktop/ms724911(v=vs.85).aspx

[83] For more information see 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

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.


oval-sc::ItemType
-id : ItemIDPattern
-status : StatusEnumeration = exists
win-sc::registry_item
-hive : EntityItemRegistryHiveType
-key : EntityItemStringType
-name : EntityItemStringType
-last_write_time : EntityItemIntType
-type : EntityItemRegistryTypeType
-value : EntityItemAnySimpleType
-windows_view : EntityItemWindowsViewType

Property	Type	Multiplicity	Nillable	Description
hive	win-sc: EntityItemRegistryHiveType	0..1	false	The hive that the registry key belongs to. This SHOULD align with the guidance provided in the MSDN documentation, which contains the list of predefined hives[85].
key	oval-sc:EntityItemStringType	0..1	true	The registry key to be collected. This property MUST NOT include the hive as it must be specified in the hive property.
name	oval-sc:EntityItemStringType	0..1	true	The name assigned to a value associated with a specific registry key. If an empty string is specified, the registry key's default value MUST be collected.

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

				This can be obtained using the RegQueryValueEx function[86].
last_write_time	oval-sc:EntityItemIntType	0..1	false	The date and time that the key or any of its value entries were last modified. This value MUST align with the FILETIME structure which contains a 64-bit number representing how many 100-nanosecond intervals have passed since January 1, 1601 (UTC)[87]. The last write time can be queried on a hive, key, or name. When collecting only information about a registry hive the last write time will be the time the hive or any of its entiries was written to. When collecting only information about a registry hive and key the last write time will be the time the key or any of its entiries was written to. When collecting only information about a registry name the last write time will be the time the name was written to. This can be obtained using the

[86] For more information see 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

				RegQueryInfoKey function[88].
type	win-sc: EntityItemRegistryTypeType	0..1	false	The type associated with the value of a hive or registry key. This can be obtained using the RegQueryValueEx function[89].
value	oval-sc: EntityItemAnySimpleType	0..*	false	The value(s) associated with a hive or registry key. The value of a hive or registry key can be obtained using the RegQueryValueEx function[90]. Please see the OVAL Language Specification [2] for more information about how datatypes are assigned to OVAL Item Entities.
windows_view	win-sc: EntityItemWindowsViewType	0..1	false	The targeted registry view[91] where the hive or registry key was collected.

2.19. win-def:EntityObjectRegistryHiveType

The `EntityObjectRegistryHiveType` defines the enumeration of possible hive types for the registry supported on Microsoft Windows platforms[92].

Enumeration Value	Description
HKEY_CLASSES_ROOT	This value indicates file types with programs and configuration data for

[88] For more information see 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

[90] For more information see 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

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

	automation (e.g. COM objects and Visual Basic Programs).
HKEY_CURRENT_CONFIG	This value indicates configuration data for the current hardware profile.
HKEY_CURRENT_USER	This value indicates the user profile of the user that is currently logged into the system.
HKEY_LOCAL_MACHINE	This value indicates information about the local system.
HKEY_USERS	This value indicates user-specific data.
<empty string>	This value indicates that no value has been specified and is permitted here to allow for an empty entity which is associated with a reference to an OVAL Variable.

2.20. win-def:EntityStateRegistryHiveType

The `EntityStateRegistryHiveType` defines the enumeration of possible hive types for the registry supported on Microsoft Windows platforms[93].

Enumeration Value	Description
HKEY_CLASSES_ROOT	This value indicates file types with programs and configuration data for automation (e.g. COM objects and Visual Basic Programs).
HKEY_CURRENT_CONFIG	This value indicates configuration data for the current hardware profile.
HKEY_CURRENT_USER	This value indicates the user profile of the user that is currently logged into the system.
HKEY_LOCAL_MACHINE	This value indicates information about the local system.
HKEY_USERS	This value indicates user-specific data.
<empty string>	This value indicates that no value has been specified and is permitted here to allow for an empty entity which is associated with a reference to an OVAL Variable.

2.21. win-sc:EntityItemRegistryHiveType

The `EntityItemRegistryHiveType` defines the enumeration of possible hive types for the registry supported on Microsoft Windows platforms[94].

Enumeration Value	Description
HKEY_CLASSES_ROOT	This value indicates file types with programs and configuration data for automation (e.g. COM objects and Visual Basic Programs).
HKEY_CURRENT_CONFIG	This value indicates configuration data for the current hardware profile.
HKEY_CURRENT_USER	This value indicates the user profile of the user that is currently logged into the system.
HKEY_LOCAL_MACHINE	This value indicates information about the local system.
HKEY_USERS	This value indicates user-specific data.
<empty string>	This value indicates that no value has been specified and is permitted here to allow for an empty entity which is associated with error and not collected conditions.

[93] For more information see 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

2.22. win-def:EntityStateRegistryTypeType

The `EntityStateRegistryTypeType` defines the types[95] associated with the values of hives and registry keys in the registry on Microsoft Windows platforms.

Enumeration Value	Description
reg_binary	This value indicates binary data in any form.
reg_dword	This value indicates a 32-bit number.
reg_expand_sz	This value indicates a null-terminated string that contains unexpanded references to environment variables.
reg_multi_sz	This value indicates an array of null-terminated strings, terminated by two null characters.
reg_none	This value indicates no defined value type.
reg_qword	This value indicates a 64-bit number.
reg_sz	This value indicates a single null-terminated string.
<empty string>	This value indicates that no value has been specified and is permitted here to allow for an empty entity which is associated with a reference to an OVAL Variable.

2.23. win-sc:EntityItemRegistryTypeType

The `EntityItemRegistryTypeType` defines the types[96] associated with the values of hives and registry keys in the registry on Microsoft Windows platforms.

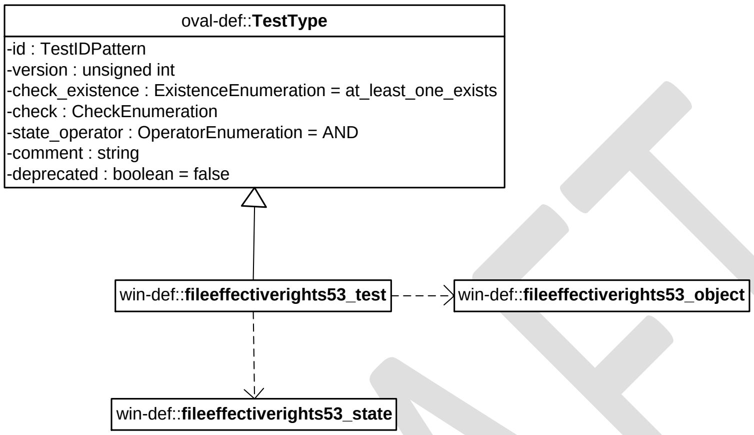
Enumeration Value	Description
reg_binary	This value indicates binary data in any form.
reg_dword	This value indicates a 32-bit number.
reg_expand_sz	This value indicates a null-terminated string that contains unexpanded references to environment variables.
reg_multi_sz	This value indicates an array of null-terminated strings, terminated by two null characters.
reg_none	This value indicates no defined value type.
reg_qword	This value indicates a 64-bit number.
reg_sz	This value indicates a single null-terminated string.
<empty string>	This value indicates that no value has been specified and is permitted here to allow for an empty entity which is associated with error and not collected conditions.

[95] For more information see 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

2.24. win-def:fileeffectiverights53_test

The `fileeffectiverights53_test` is used to make assertions about the effective rights of files on Microsoft Windows operating systems[97]. The `fileeffectiverights53_test` MUST reference one `fileeffectiverights53_object` and zero or more `fileeffectiverights53_states`.


oval-def::TestType
-id : TestIDPattern
-version : unsigned int
-check_existence : ExistenceEnumeration = at_least_one_exists
-check : CheckEnumeration
-state_operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::fileeffectiverights53_test
win-def::fileeffectiverights53_object
win-def::fileeffectiverights53_state

2.24.1. Known Supported Platforms

Comment [DJH2]: We probably want to consider adding windows 2000, windows server 2003, windows server 2008, and windows server 2008 r2.

- Windows XP
- Windows Vista
- Windows 7

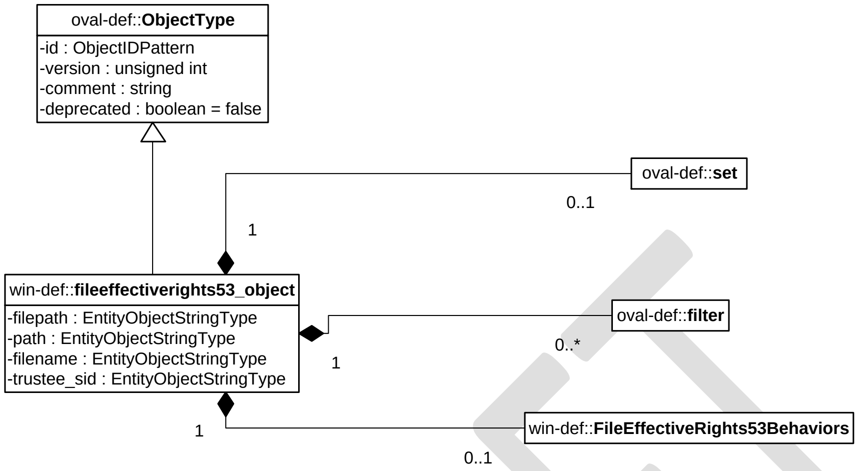
2.25. win-def:fileeffectiverights53_object

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

[97] For more information see http://msdn.microsoft.com/en-us/library/windows/desktop/aa364399(v=vs.85).aspx , http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx, and http://technet.microsoft.com/en-us/library/bb727008.aspx

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

directiories and all file types as defined in the EntityStateFileTypeType


oval-def::ObjectType
-id : ObjectIDPattern
-version : unsigned int
-comment : string
-deprecated : boolean = false
oval-def::set
0..1
1
win-def::fileeffectiverights53_object
-filepath : EntityObjectStringType
-path : EntityObjectStringType
-filename : EntityObjectStringType
-trustee_sid : EntityObjectStringType
oval-def::filter
0..*
1
win-def::FileEffectiveRights53Behaviors
1
0..1

Property	Type	Multiplicity	Nillable	Description
Set	oval-def:set	0..1	false	Enables the expression of complex `fileeffectiverights53_objects` that are the result of logically combining and filtering the `fileeffectiverights53_items` that are identified by one or more `fileeffectiverights53_objects`. The behaviors, filepath, path, filename, trustee_sid, and filter properties MUST NOT be specified when this property is specified. Please see the OVAL Language Specification [2] for additional information.
behaviors	win-def: FileEffectiveRights53Behaviors	0..1	false	Specifies the behaviors that direct how the `fileeffectiverights53_object` collects `fileeffectiverights53_items` from the

				system.
filepath	oval-def: EntityObjectStringType	0..1	false	The absolute path to a file on the system. The absolute path SHOULD align with the guidance provided in the MSDN documentation[99]. A directory MUST NOT be specified for this property. The max_depth and recurse_direction behaviors MUST NOT be used in conjunction with this property as they are reserved for use with the path and filename properties.
path	oval-def: EntityObjectStringType	0..1	false	The directory component of the absolute path to a directory or file on the system. The path component SHOULD align with the guidance provided in the MSDN documentation[100]. The filepath property MUST NOT be specified when this property is specified.
filename	oval-def: EntityObjectStringType	0..1	true	The name of a file to evaluate. A filename MUST NOT contain the characters in the set { /, \, ?, |, >, :, *}. The filename SHOULD also align with the guidance provided in the MSDN

[99] For more information see 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

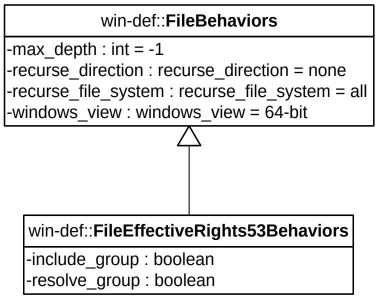
				documentation, as there are more conventions when naming files beyond the characters listed above[101]. **xsi:nil="true"** indicates that the `fileeffectiverights53_object` MUST collect the set of directories specified by the path entity. In addition, a value for the filename entity MUST NOT be specified.
trustee_sid	oval-def: EntityObjectStringType	1..1	false	The unique security identifier associated with a user account, group account, or logon session. If an operation other than equals is used to identify the matching trustees, then the resulting matches MUST be limited to the trustees explicitly referenced in the file or directory's security descriptor[102].
filter	oval-def:filter	0..*	false	Allows for the explicit inclusion or exclusion of `fileeffectiverights53_items` from the set of `fileeffectiverights53_items` collected by a `fileeffectiverights53_object`. Please see the OVAL Language Specification [2] for additional information.

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

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.


win-def::**FileBehaviors**
-max_depth : int = -1
-recurse_direction : recurse_direction = none
-recurse_file_system : recurse_file_system = all
-windows_view : windows_view = 64-bit
win-def::**FileEffectiveRights53Behaviors**
-include_group : boolean
-resolve_group : boolean

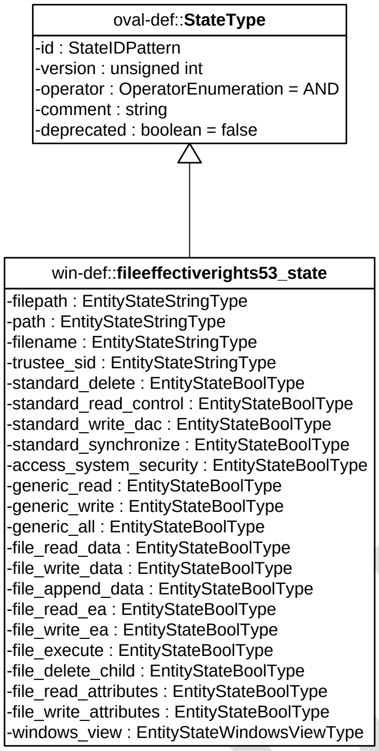
Attribute	Type	Possible Values	Description
include_group	boolean	*'true'* *'false'*	Defines whether or not the group SID should be collected when the trustee_sid property specifies a group SID. *'true'*: The group SID MUST be collected when the trustee_sid property specifies a group SID. *'false'*: The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

			groups should also be resolved and any valid domain accounts that are members should also be included. The intent of this behavior is to end up with a list of all individual users from that system that make up the group once everything has been resolved. *'true'*: The members of a group SID MUST be resolved and collected. 'false': The members of a group SID MUST NOT be resolved or collected. **Default Value: false**

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 permissions[103].

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


oval-def::StateType
-id : StateIDPattern
-version : unsigned int
-operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::fileeffectiverights53_state
-filepath : EntityStateStringType
-path : EntityStateStringType
-filename : EntityStateStringType
-trustee_sid : EntityStateStringType
-standard_delete : EntityStateBoolType
-standard_read_control : EntityStateBoolType
-standard_write_dac : EntityStateBoolType
-standard_synchronize : EntityStateBoolType
-access_system_security : EntityStateBoolType
-generic_read : EntityStateBoolType
-generic_write : EntityStateBoolType
-generic_all : EntityStateBoolType
-file_read_data : EntityStateBoolType
-file_write_data : EntityStateBoolType
-file_append_data : EntityStateBoolType
-file_read_ea : EntityStateBoolType
-file_write_ea : EntityStateBoolType
-file_execute : EntityStateBoolType
-file_delete_child : EntityStateBoolType
-file_read_attributes : EntityStateBoolType
-file_write_attributes : EntityStateBoolType
-windows_view : EntityStateWindowsViewType

Property	Type	Multiplicity	Nillable	Description
filepath	oval-def: EntityStateStringType	0..1	false	The absolute path to a file on the system. The absolute path SHOULD align with the guidance provided in the MSDN documentation[104]. A directory MUST NOT be specified for this property. The max_depth and recurse_direction

[104] For more information see 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	The directory component of the absolute path to a directory or file on the system. The path component SHOULD align with the guidance provided in the MSDN documentation[105]. The filepath property MUST NOT be specified when this property is specified.
filename	oval-def: EntityStateStringType	0..1	false	The name of a file to evaluate. A filename MUST NOT contain the characters in the set { /, \, ?, |, >, :, *}. The filename SHOULD also align with the guidance provided in the MSDN documentation, as there are more conventions when naming files beyond the characters listed above[106].

[105] For more information see 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

[108] For more information see 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

[110] For more information see 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

				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

[113] For more information see 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

[115] For more information see 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

[117] For more information see 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

[119] For more information see 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

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

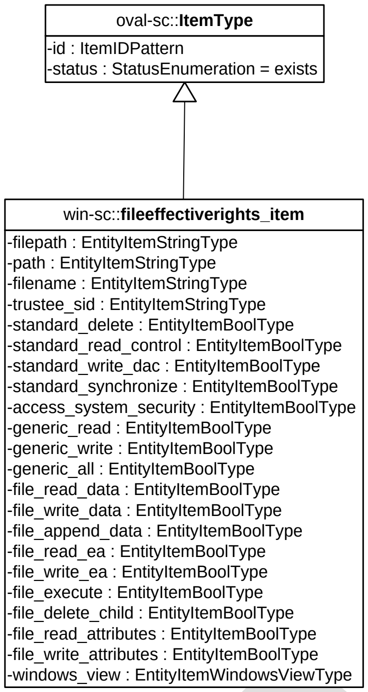
	EntityStateBoolType			write extended attributes[122].
file_execute	oval-def: EntityStateBoolType	0..1	false	Grants the right to execute a file, or if a directory, the right to traverse the directory[123].
file_delete_child	oval-def: EntityStateBoolType	0..1	false	Right to delete a directory and all the 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
[123] For more information see 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
[125] For more information see 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

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


oval-sc::ItemType
-id : ItemIDPattern
-status : StatusEnumeration = exists
win-sc::fileeffectiverights_item
-filepath : EntityItemStringType
-path : EntityItemStringType
-filename : EntityItemStringType
-trustee_sid : EntityItemStringType
-standard_delete : EntityItemBoolType
-standard_read_control : EntityItemBoolType
-standard_write_dac : EntityItemBoolType
-standard_synchronize : EntityItemBoolType
-access_system_security : EntityItemBoolType
-generic_read : EntityItemBoolType
-generic_write : EntityItemBoolType
-generic_all : EntityItemBoolType
-file_read_data : EntityItemBoolType
-file_write_data : EntityItemBoolType
-file_append_data : EntityItemBoolType
-file_read_ea : EntityItemBoolType
-file_write_ea : EntityItemBoolType
-file_execute : EntityItemBoolType
-file_delete_child : EntityItemBoolType
-file_read_attributes : EntityItemBoolType
-file_write_attributes : EntityItemBoolType
-windows_view : EntityItemWindowsViewType

Property	Type	Multiplicity	Nillable	Description
filepath	oval-sc: EntityItemStringType	0..1	false	The absolute path to a file on the system. The absolute path SHOULD align with the guidance provided in the MSDN documentation[128]. A directory MUST NOT be specified for this property. The max_depth and recurse_direction behaviors MUST NOT be used in conjunction with this property as they are reserved for use with the path and

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

				filename properties.
path	oval-sc: EntityItemStringType	0..1	false	The directory component of the absolute path to a directory or file on the system. The path component SHOULD align with the guidance provided in the MSDN documentation[129]. The filepath property MUST NOT be specified when this property is specified.
filename	oval-sc: EntityItemStringType	0..1	true	The name of a file to evaluate. A filename MUST NOT contain the characters in the set { /, \, ?, |, >, :, *}. The filename SHOULD also align with the guidance provided in the MSDN documentation, as there are more conventions when naming files beyond the characters listed above[130].
trustee_sid	oval-sc: EntityItemStringType	0..1	false	The unique security identifier associated with a user account, group account, or logon session. If an operation other than equals is used to identify the matching trustees, then the resulting matches MUST be limited to the trustees explicitly referenced in the file or directory's security descriptor[131].

[129] For more information see 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

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
[133] For more information see 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
[135] For more information see 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
[137] For more information see 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
[139] For more information see 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
[141] For more information see 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
[143] For more information see 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

[145] For more information see 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

[147] For more information see 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

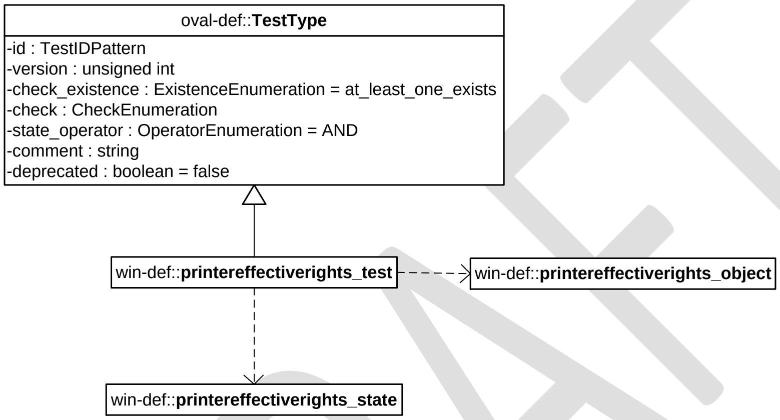
[149] For more information see http://msdn.microsoft.com/en-us/library/windows/desktop/gg258116(v=vs.85).aspx

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

[151] For more information see 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 printers[152]. The printereffectiverights53_test MUST reference one printereffectiverights53_object and zero or more printereffectiverights53_states.


oval-def::TestType
-id : TestIDPattern
-version : unsigned int
-check_existence : ExistenceEnumeration = at_least_one_exists
-check : CheckEnumeration
-state_operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::printereffectiverights_test
win-def::printereffectiverights_object
win-def::printereffectiverights_state

2.29.1. Known Supported Platforms

- Windows XP
- Windows Vista
- Windows 7

Comment [DJH3]: We probably want to consider adding windows 2000, windows server 2003, windows server 2008, and windows server 2008 r2.

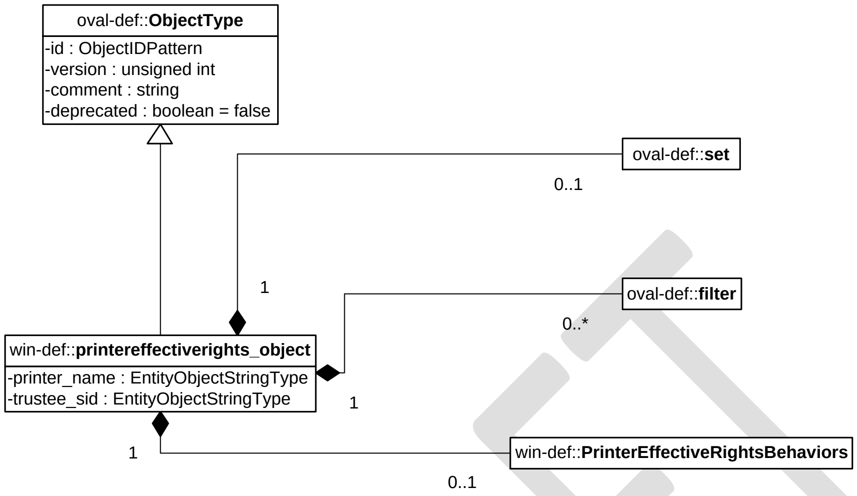
2.30. win-def:printereffectiverights_object

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

[152] For more information see 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

effective rights object.


oval-def::**ObjectType**
-id : ObjectIDPattern
-version : unsigned int
-comment : string
-deprecated : boolean = false
oval-def::**set**
0..1
1
oval-def::**filter**
0..*
win-def::**printereffectiverights_object**
-printer_name : EntityObjectStringType
-trustee_sid : EntityObjectStringType
1
1
win-def::**PrinterEffectiveRightsBehaviors**
0..1

Property	Type	Multiplicity	Nillable	Description
set	oval-def:set	0..1	false	Enables the expression of complex printereffectiverights_objects that are the result of logically combining and filtering the printereffectiverights_items that are identified by one or more printereffectiverights _objects.
behaviors	win-def: PrinterEffectiveRightsBehaviors	0..1	false	Specifies the behaviors that direct how the printereffectiverights_object collects printereffectiverights_items from the system.
printer_name	oval-def: EntityObjectStringType	0..1	false	A printer that a user may have rights on. The printer name SHOULD align with the guidance provided in the MSDN documentation.
trustee_sid	oval-def:	0..1	true	The unique SID associated

	EntityObjectStringType			with a user, group, system, or program (such as a Windows service). If an operation other than equals is used to identify matching trustees, such as not equal or pattern match, then the resulting matches SHALL be limited to only the trustees referenced in the printer's Security Descriptor[154].
filter	oval-def:filter [2]	0..*	false	Allows for the explicit inclusion or exclusion of `printereffectiverights_items` from the set of `printereffectiverights_items` collected by a `printereffectiverights_object`. Please see the OVAL Language Specification [2] for additional information.

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.

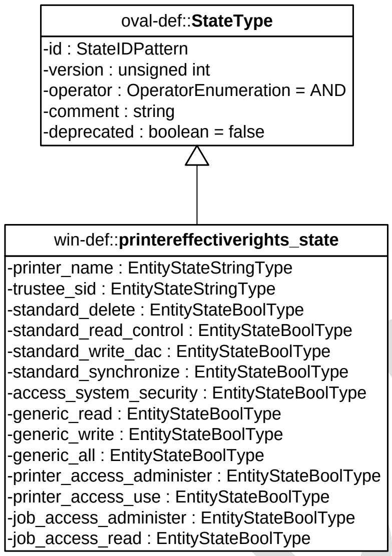
Attribute	Type	Possible Values	Description
include_group	bool	*'true'* *'false'*	Defines whether or not the group SID should be collected when the trustee_sid property specifies a group SID.

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

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

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.


oval-def::StateType
-id : StateIDPattern
-version : unsigned int
-operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::printereffectiverights_state
-printer_name : EntityStateStringType
-trustee_sid : EntityStateStringType
-standard_delete : EntityStateBoolType
-standard_read_control : EntityStateBoolType
-standard_write_dac : EntityStateBoolType
-standard_synchronize : EntityStateBoolType
-access_system_security : EntityStateBoolType
-generic_read : EntityStateBoolType
-generic_write : EntityStateBoolType
-generic_all : EntityStateBoolType
-printer_access_administer : EntityStateBoolType
-printer_access_use : EntityStateBoolType
-job_access_administer : EntityStateBoolType
-job_access_read : EntityStateBoolType

Property	Type	Multiplicity	Nillable	Description
printer_name	oval-def: EntityStateStringType	0..1	false	A printer that a user may have rights on. The printer name SHOULD align with the guidance provided in the MSDN documentation.
trustee_sid	oval-def: EntityStateStringType	0..1	false	The unique SID associated with a user, group, system, or program (such as a Windows service)[155].
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

[156] For more information see 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, amd setting the printer status[167].

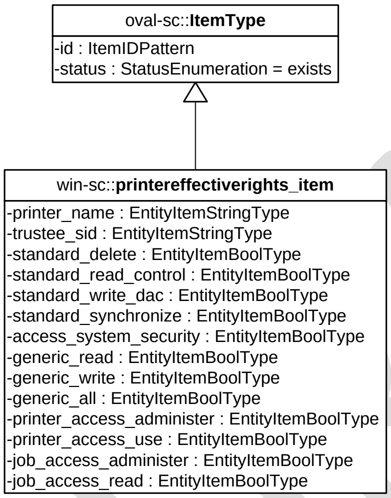
[157] For more information see http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx
[158] For more information see http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx
[159] For more information see http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx
[160] For more information see http://msdn.microsoft.com/en-us/library/windows/desktop/aa379607(v=vs.85).aspx
[161] For more information see 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
[163] For more information see 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
[165] For more information see 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
[167] For more information see 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_administer	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.


oval-sc::ItemType
-id : ItemIDPattern
-status : StatusEnumeration = exists
win-sc::printereffectiverights_item
-printer_name : EntityItemStringType
-trustee_sid : EntityItemStringType
-standard_delete : EntityItemBoolType
-standard_read_control : EntityItemBoolType
-standard_write_dac : EntityItemBoolType
-standard_synchronize : EntityItemBoolType
-access_system_security : EntityItemBoolType
-generic_read : EntityItemBoolType
-generic_write : EntityItemBoolType
-generic_all : EntityItemBoolType
-printer_access_administer : EntityItemBoolType
-printer_access_use : EntityItemBoolType
-job_access_administer : EntityItemBoolType
-job_access_read : EntityItemBoolType

Property	Type	Multiplicity	Nillable	Description
printer_name	oval-sc: EntityItemStringType	0..1	false	A printer that a user may have rights on. The printer name SHOULD align with the guidance provided in the MSDN documentation.

[168] For more information see 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

[170] For more information see 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

[172] For more information see 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

[174] For more information see 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

[176] For more information see 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

[178] For more information see 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

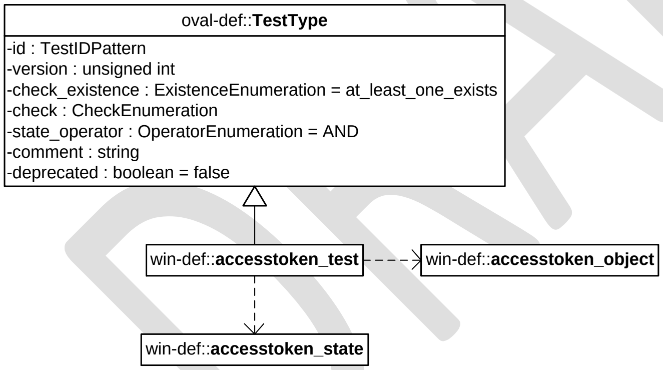
[180] For more information see http://msdn.microsoft.com/en-us/library/windows/desktop/aa446632(v=VS.85).aspx

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

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, amd 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:accesstoken_test

The `accesstoken_test` is used to make assertions about the properties of Windows access tokens as well as individual privileges and rights associated with them[187]. The `accesstoken_test` MUST reference one `accesstoken_object` and zero or more `accesstoken_states`.


oval-def::TestType
-id : TestIDPattern
-version : unsigned int
-check_existence : ExistenceEnumeration = at_least_one_exists
-check : CheckEnumeration
-state_operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::accesstoken_test
win-def::accesstoken_object
win-def::accesstoken_state

2.34.1. Known Supported Platforms

- Windows XP

Comment [DJH4]: We probably want to consider adding windows 2000, windows server 2003, windows server 2008, and windows server 2008 r2.

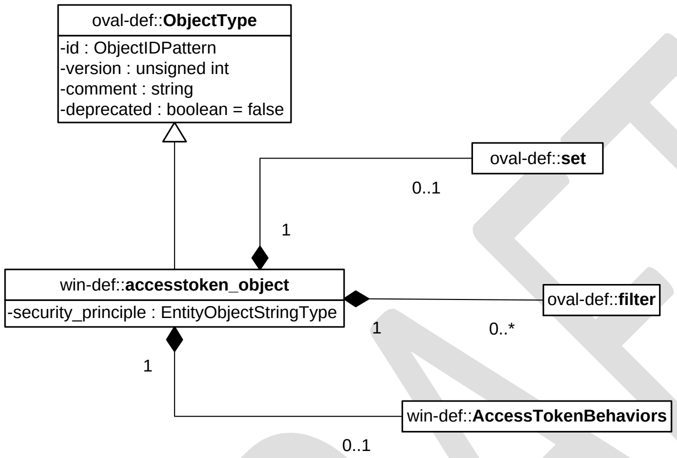
[182] For more information see http://msdn.microsoft.com/en-us/library/windows/desktop/dd162751(v=vs.85).aspx
[183] For more information see http://msdn.microsoft.com/en-us/library/windows/desktop/dd145082(v=vs.85).aspx
[184] For more information see http://msdn.microsoft.com/en-us/library/windows/desktop/dd162751(v=vs.85).aspx
[185] For more information see http://msdn.microsoft.com/en-us/library/cc244650(v=PROT.10).aspx
[186] For more information see 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

- 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 token[188], whose associated information should be collected and represented as `accesstoken_items`.


oval-def::ObjectType
-id : ObjectIDPattern
-version : unsigned int
-comment : string
-deprecated : boolean = false
oval-def::set
0..1
1
win-def::accesstoken_object
-security_principle : EntityObjectStringType
oval-def::filter
1
0..*
1
win-def::AccessTokenBehaviors
0..1

Property	Type	Multiplicity	Nillable	Description
set	oval-def:set	0..1	false	Enables the expression of complex `accesstoken_objects` that are the result of logically combining and filtering the `accesstoken_items` that are identified by one or more `accesstoken_objects`.
behaviors	win-def: AccesstokenBehaviors	0..1	false	Specifies the behaviors that direct how the `accesstoken_object` collects `accesstoken_items` from the system.
security_principle	oval-def: EntityObjectStringType	0..1	false	The access token being specified. Security principals include users or groups with either local or domain

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

				accounts, and computer accounts created when a computer joins a domain. In Windows, security principals are case-insensitive. As a result, it is recommended that the case-insensitive operations are used for this entity.
filter	oval-def:filter [2]	0..*	false	Allows for the explicit inclusion or exclusion of `accesstoken_items` from the set of `accesstoken_items` collected by a `accesstoken_object`. Please see the OVAL Language Specification [2] for additional information.

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.

Attribute	Type	Possible Values	Description
include_group	bool	*'true'* *'false'*	Defines whether or not the group SID should be collected when the trustee_sid property specifies a group SID. *'true'*: The group SID MUST be collected when the trustee_sid property specifies a group SID. *'false'*: The group SID MUST NOT be collected when the trustee_sid

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

2.37. win-def:accesstoken_state

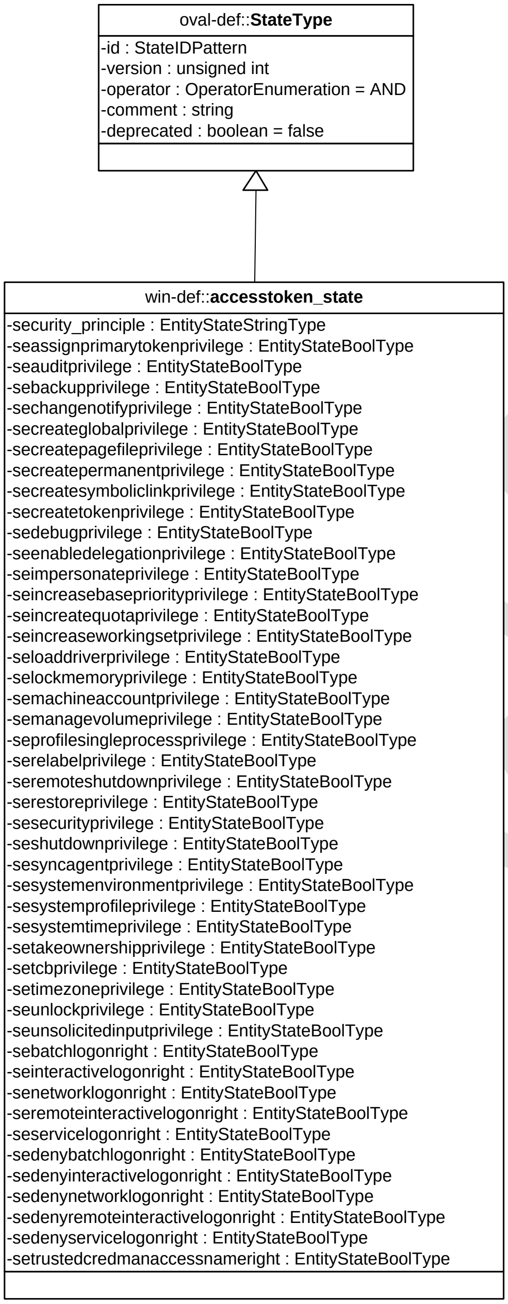
The `accesstoken_state` construct is used by an `accesstoken_test` to specify the information that can be used to evaluate the specified access tokens associated with a given `accesstoken_object`. All attributes ending in "privilege" are considered access token privileges[189],

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

and all attributes ending in "right", with the exception of setrustedcredmanaccessnameright, which is a privilege[190], are access token rights[191].

[190] For more information see 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


oval-def::**StateType**
-id : StateIDPattern
-version : unsigned int
-operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::**accesstoken_state**
-security_principle : EntityStateStringType
-seassignprimarytokenprivilege : EntityStateBoolType
-seauditprivilege : EntityStateBoolType
-sebackupprivilege : EntityStateBoolType
-sechangenotifyprivilege : EntityStateBoolType
-secreateglobalprivilege : EntityStateBoolType
-secreatepagefileprivilege : EntityStateBoolType
-secreatepermanentprivilege : EntityStateBoolType
-secreatesymboliclinkprivilege : EntityStateBoolType
-secreatetokenprivilege : EntityStateBoolType
-sedebugprivilege : EntityStateBoolType
-seenabledelegationprivilege : EntityStateBoolType
-seimpersonateprivilege : EntityStateBoolType
-seincreasebasepriorityprivilege : EntityStateBoolType
-seincreatequotaprivilege : EntityStateBoolType
-seincreaseworkingsetprivilege : EntityStateBoolType
-seloaddriverprivilege : EntityStateBoolType
-selockmemoryprivilege : EntityStateBoolType
-semachineaccountprivilege : EntityStateBoolType
-semanagevolumeprivilege : EntityStateBoolType
-seprofilesingleprocessprivilege : EntityStateBoolType
-serelabelprivilege : EntityStateBoolType
-seremoteshutdownprivilege : EntityStateBoolType
-serestoreprivilege : EntityStateBoolType
-sesecurityprivilege : EntityStateBoolType
-seshutdownprivilege : EntityStateBoolType
-sesyncagentprivilege : EntityStateBoolType
-sesystemenvironmentprivilege : EntityStateBoolType
-sesystemprofileprivilege : EntityStateBoolType
-sesystemtimeprivilege : EntityStateBoolType
-setakeownershipprivilege : EntityStateBoolType
-setcbprivilege : EntityStateBoolType
-setimezoneprivilege : EntityStateBoolType
-seunlockprivilege : EntityStateBoolType
-seunsolicitedinputprivilege : EntityStateBoolType
-sebatchlogonright : EntityStateBoolType
-seinteractivelogonright : EntityStateBoolType
-senetworklogonright : EntityStateBoolType
-seremoteinteractivelogonright : EntityStateBoolType
-seservicelogonright : EntityStateBoolType
-sedenybatchlogonright : EntityStateBoolType
-sedenyinteractivelogonright : EntityStateBoolType
-sedenynetworklogonright : EntityStateBoolType
-sedenyremoteinteractivelogonright : EntityStateBoolType
-sedenyservicelogonright : EntityStateBoolType
-setrustedcredmanaccessnameright : EntityStateBoolType

Property	Type	Multiplicity	Nillable	Description
security_principle	oval-def: EntityStateStringType	0..1	false	Identifies an access token to test for. Security principals include users or groups with either local or domain accounts, and computer accounts created when a computer joins a domain. In Windows, security principals are case-insensitive. As a result, it is recommended that the case-insensitive operations are used for this entity.
seassignprimarytokenprivilege	oval-def: EntityStateBoolType	0..1	false	Gives the user the privilege to replace a process-level token.
seauditprivilege	oval-def: EntityStateBoolType	0..1	false	Gives the user the privilege to generate security audits.
sebackupprivilege	oval-def: EntityStateBoolType	0..1	false	Gives the user the privilege to back up files and directories. If this privilege is held, the READ_CONTROL, ACCESS_SYSTEM_SECURITY, FILE_GENERIC_READ, and FILE_TRAVERSE rights are granted.
sechangenotifyprivilege	oval-def: EntityStateBoolType	0..1	false	Gives the user the privilege to bypass traverse checking. This privilege is enabled by default for all users.
secreateglobalprivilege	oval-def: EntityStateBoolType	0..1	false	Gives the user the privilege to create global objects. It is enabled by default for administrators, services, and the local system account.
secreatepagefileprivilege	oval-def: EntityStateBoolType	0..1	false	Gives the user the privilege to create a pagefile.
secreatepermanentprivilege	oval-def: EntityStateBoolType	0..1	false	Gives the user the privilege to create permanent shared object.
secreatesymboliclinkprivilege	oval-def: EntityStateBoolType	0..1	false	Gives the user the privilege to create symbolic links.
secreatetokenprivilege	oval-def: EntityStateBoolType	0..1	false	Gives the user the privilege to create a token object.

sedebugprivilege	oval-def: EntityStateBoolType	0..1	false	Gives the user the privilege to debug programs, especially to debug and adjust the memory of a process owned by another account.
seenabledelegationprivilege	oval-def: EntityStateBoolType	0..1	false	Gives the user the privilege to enable computer and user accounts to be trusted for delegation.
seimpersonateprivilege	oval-def: EntityStateBoolType	0..1	false	Gives the user the privilege to impersonate a client after authentication.
seincreasebasepriorityprivilege	oval-def: EntityStateBoolType	0..1	false	Gives the user the privilege to increase scheduling priority.
seincreasequotaprivilege	oval-def: EntityStateBoolType	0..1	false	Gives the user the privilege to adjust memory quotas for a process.
seincreaseworkingsetprivilege	oval-def: EntityStateBoolType	0..1	false	Gives the user the privilege to increase a process working set.
seloaddriverprivilege	oval-def: EntityStateBoolType	0..1	false	Gives the user the privilege to load and unload device drivers.
selockmemoryprivilege	oval-def: EntityStateBoolType	0..1	false	Gives the user the privilege to lock pages in memory.
semachineaccountprivilege	oval-def: EntityStateBoolType	0..1	false	Gives the user the privilege to add workstations to domain.
Semanagevolumeprivilege	oval-def: EntityStateBoolType	0..1	false	Gives the user the privilege to manage the files on a volume.
seprofilesingleprocessprivilege	oval-def: EntityStateBoolType	0..1	false	Gives the user the privilege to profile a single process.
serelabelprivilege	oval-def: EntityStateBoolType	0..1	false	Gives the user the privilege to modify an object label.
seremoteshutdownprivilege	oval-def: EntityStateBoolType	0..1	false	Gives the user the privilege to force shutdown from a remote system.
serestoreprivilege	oval-def: EntityStateBoolType	0..1	false	Gives the user the privilege to restore files and directories. The following access rights are granted if this privilege is held: WRITE_DAC, WRITE_OWNER, ACCESS_SYSTEM_SECURITY, FILE_GENERIC_WRITE, FILE_ADD_FILE,

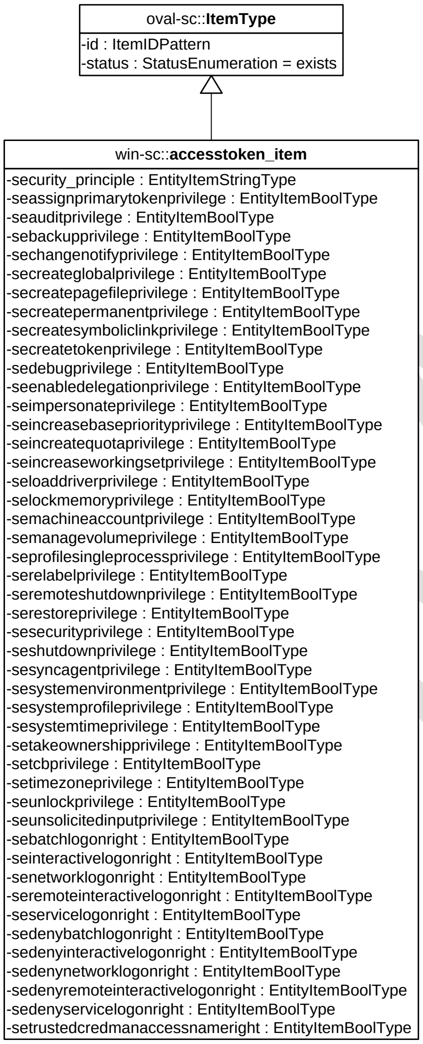
				FILE_ADD_SUBDIRECTORY, and DELETE.
sesecurityprivilege	oval-def: EntityStateBoolType	0..1	false	Gives the user the privilege to manage auditing and security log.
seshutdownprivilege	oval-def: EntityStateBoolType	0..1	false	Gives the user the privilege to shut down the system.
sesyncagentprivilege	oval-def: EntityStateBoolType	0..1	false	Gives the user the privilege to synchronize directory service data. This privilege enables the holder to read all objects and properties in the directory, regardless of the protection on the objects and properties. By default, it is assigned to the Administrator and LocalSystem accounts on domain controllers.
sesystemenvironmentprivilege	oval-def: EntityStateBoolType	0..1	false	Gives the user the privilege to modify firmware environment values, especially to modify the nonvolatile RAM of systems that use this type of memory to store configuration information.
sesystemprofileprivilege	oval-def: EntityStateBoolType	0..1	false	Gives the user the privilege to profile system performance.
sesystemtimeprivilege	oval-def: EntityStateBoolType	0..1	false	Gives the user the privilege to change the system time.
setakeownershipprivilege	oval-def: EntityStateBoolType	0..1	false	Gives the user the privilege to take ownership of files or other objects. It allows the owner value to be set only to those values that the holder may legitimately assign as the owner of an object.
setcbprivilege	oval-def: EntityStateBoolType	0..1	false	Gives the user the privilege to act as part of the operating system, i.e. as part of the Trusted Computer Base (TCB). Some trusted protected subsystems are granted this

				privilege.
setimezoneprivilege	oval-def: EntityStateBoolType	0..1	false	Gives the user the privilege to change the time zone.
seundockprivilege	oval-def: EntityStateBoolType	0..1	false	Gives the user the privilege to remove the computer from a docking station.
seunsolicitedinputprivilege	oval-def: EntityStateBoolType	0..1	false	Allows the user to read unsolicited input from a terminal device.
sebatchlogonright	oval-def: EntityStateBoolType	0..1	false	Grants the right for an account to log on using the batch logon type.
seinteractivelogonright	oval-def: EntityStateBoolType	0..1	false	Grants the right for an account to log on using the interactive logon type.
senetworklogonright	oval-def: EntityStateBoolType	0..1	false	Grants the right for an account to log on using the network logon type.
seremoteinteractivelogonright	oval-def: EntityStateBoolType	0..1	false	Grants the right for an account to log on remotely using the interactive logon type.
seservicelogonright	oval-def: EntityStateBoolType	0..1	false	Grants the right for an account to log on using the service logon type.
sedenybatchlogonright	oval-def: EntityStateBoolType	0..1	false	Denies the right for an account to log on using the batch logon type.
sedenyinteractivelogonright	oval-def: EntityStateBoolType	0..1	false	Denies the right for an account to log on using the interactive logon type.
sedenynetworklogonright	oval-def: EntityStateBoolType	0..1	false	Denies the right for an account to log on using the network logon type.
sedenyremoteinteractivelogonright	oval-def: EntityStateBoolType	0..1	false	Denies the right for an account to log on remotely using the interactive logon type.
sedenyservicelogonright	oval-def: EntityStateBoolType	0..1	false	Denies the right for an account to log on using the service logon type.
setrustedcredmanaccessnameright	oval-def: EntityStateBoolType	0..1	false	Gives the user the privilege to access Credential Manager as a trusted caller. NOTE: This is a privilege (referred to as SE_TRUSTED_CREDMAN_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 privileges[192], and all attributes ending in "right", with the exception of setrustedcredmanaccessnameright, which is a privilege[193], are access token rights[194].


oval-sc::ItemType
-id : ItemIDPattern
-status : StatusEnumeration = exists
win-sc::accesstoken_item
-security_principle : EntityItemStringType
-seassignprimarytokenprivilege : EntityItemBoolType
-seauditprivilege : EntityItemBoolType
-sebackupprivilege : EntityItemBoolType
-sechangenotifyprivilege : EntityItemBoolType
-secreateglobalprivilege : EntityItemBoolType
-secreatepagefileprivilege : EntityItemBoolType
-secreatepermanentprivilege : EntityItemBoolType
-secreatesymboliclinkprivilege : EntityItemBoolType
-secreatetokenprivilege : EntityItemBoolType
-sedebugprivilege : EntityItemBoolType
-seenabledelegationprivilege : EntityItemBoolType
-seimpersonateprivilege : EntityItemBoolType
-seincreasebasepriorityprivilege : EntityItemBoolType
-seincreasequotaprivilege : EntityItemBoolType
-seincreaseworkingsetprivilege : EntityItemBoolType
-seloaddriverprivilege : EntityItemBoolType
-selockmemoryprivilege : EntityItemBoolType
-semachineaccountprivilege : EntityItemBoolType
-semanagevolumeprivilege : EntityItemBoolType
-seprofilesingleprocessprivilege : EntityItemBoolType
-serelabelprivilege : EntityItemBoolType
-seremoteshutdownprivilege : EntityItemBoolType
-serestoreprivilege : EntityItemBoolType
-sesecurityprivilege : EntityItemBoolType
-seshutdownprivilege : EntityItemBoolType
-sesyncagentprivilege : EntityItemBoolType
-sesystemenvironmentprivilege : EntityItemBoolType
-sesystemprofileprivilege : EntityItemBoolType
-sesystemtimeprivilege : EntityItemBoolType
-setakeownershipprivilege : EntityItemBoolType
-setcbprivilege : EntityItemBoolType
-setimezoneprivilege : EntityItemBoolType
-seunlockprivilege : EntityItemBoolType
-seunsolicitedinputprivilege : EntityItemBoolType
-sebatchlogonright : EntityItemBoolType
-seinteractivelogonright : EntityItemBoolType
-senetworklogonright : EntityItemBoolType
-seremoteinteractivelogonright : EntityItemBoolType
-seservicelogonright : EntityItemBoolType
-sedenybatchlogonright : EntityItemBoolType
-sedenyinteractivelogonright : EntityItemBoolType
-sedenynetworklogonright : EntityItemBoolType
-sedenyremoteinteractivelogonright : EntityItemBoolType
-sedenyservicelogonright : EntityItemBoolType
-setrustedcredmanaccessnameright : EntityItemBoolType

[192] For more information see 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

Property	Type	Multiplicity	Nillable	Description
security_principle	oval-sc: EntityItemStringType	0..1	false	Identifies an access token to test for. Security principals include users or groups with either local or domain accounts, and computer accounts created when a computer joins a domain. In Windows, security principals are case-insensitive. As a result, it is recommended that the case-insensitive operations are used for this entity.
seassignprimarytokenprivilege	oval-sc:EntityItemBoolType	0..1	false	Gives the user the privilege to replace a process-level token.
seauditprivilege	oval-sc:EntityItemBoolType	0..1	false	Gives the user the privilege to generate security audits.
sebackupprivilege	oval-sc:EntityItemBoolType	0..1	false	Gives the user the privilege to back up files and directories. If this privilege is held, the READ_CONTROL, ACCESS_SYSTEM_SECURITY, FILE_GENERIC_READ, and FILE_TRAVERSE rights are granted.
sechangenotifyprivilege	oval-sc:EntityItemBoolType	0..1	false	Gives the user the privilege to bypass traverse checking. This privilege is enabled by default for all users.
secreateglobalprivilege	oval-sc:EntityItemBoolType	0..1	false	Gives the user the privilege to create global objects. It is enabled by default for administrators, services, and the local system account.
secreatepagefileprivilege	oval-sc:EntityItemBoolType	0..1	false	Gives the user the privilege to create a pagefile.

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

secreatepermanentprivilege	oval-sc:EntityItemBoolType	0..1	false	Gives the user the privilege to create permanent shared object.
secreatesymboliclinkprivilege	oval-sc:EntityItemBoolType	0..1	false	Gives the user the privilege to create symbolic links.
secreatetokenprivilege	oval-sc:EntityItemBoolType	0..1	false	Gives the user the privilege to create a token object.
sedebugprivilege	oval-sc:EntityItemBoolType	0..1	false	Gives the user the privilege to debug programs, especially to debug and adjust the memory of a process owned by another account.
seenabledelegationprivilege	oval-sc:EntityItemBoolType	0..1	false	Gives the user the privilege to enable computer and user accounts to be trusted for delegation.
seimpersonateprivilege	oval-sc:EntityItemBoolType	0..1	false	Gives the user the privilege to impersonate a client after authentication.
seincreasebasepriorityprivilege	oval-sc:EntityItemBoolType	0..1	false	Gives the user the privilege to increase scheduling priority.
seincreasequotaprivilege	oval-sc:EntityItemBoolType	0..1	false	Gives the user the privilege to adjust memory quotas for a process.
seincreaseworkingsetprivilege	oval-sc:EntityItemBoolType	0..1	false	Gives the user the privilege to increase a process working set.
Seloaddriverprivilege	oval-sc:EntityItemBoolType	0..1	false	Gives the user the privilege to load and unload device drivers.
selockmemoryprivilege	oval-sc:EntityItemBoolType	0..1	false	Gives the user the privilege to lock pages in memory.
semachineaccountprivilege	oval-sc:EntityItemBoolType	0..1	false	Gives the user the privilege to add workstations to domain.
semanagevolumeprivilege	oval-sc:EntityItemBoolType	0..1	false	Gives the user the privilege to manage the files on a volume.
seprofilesingleprocessprivilege	oval-sc:EntityItemBoolType	0..1	false	Gives the user the privilege to profile a single process.
serelabelprivilege	oval-sc:EntityItemBoolType	0..1	false	Gives the user the privilege to modify an object label.
seremoteshutdownprivilege	oval-sc:EntityItemBoolType	0..1	false	Gives the user the privilege to force shutdown from a remote system.
serestoreprivilege	oval-sc:EntityItemBoolType	0..1	false	Gives the user the privilege to restore files and directories.

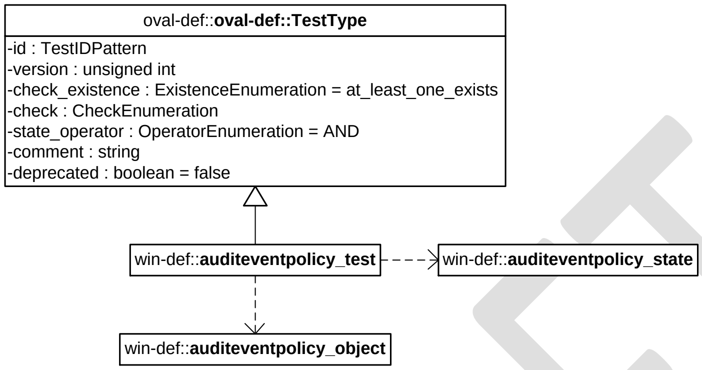
				The following access rights are granted if this privilege is held: WRITE_DAC, WRITE_OWNER, ACCESS_SYSTEM_SECURITY, FILE_GENERIC_WRITE, FILE_ADD_FILE, FILE_ADD_SUBDIRECTORY, and DELETE.
sesecurityprivilege	oval-sc:EntityItemBoolType	0..1	false	Gives the user the privilege to manage auditing and security log.
seshutdownprivilege	oval-sc:EntityItemBoolType	0..1	false	Gives the user the privilege to shut down the system.
sesyncagentprivilege	oval-sc:EntityItemBoolType	0..1	false	Gives the user the privilege to synchronize directory service data. This privilege enables the holder to read all objects and properties in the directory, **regardless** of the protection on the objects and properties. By default, it is assigned to the Administrator and LocalSystem accounts on domain controllers.
sesystemenvironmentprivilege	oval-sc:EntityItemBoolType	0..1	false	Gives the user the privilege to modify firmware environment values, especially to modify the nonvolatile RAM of systems that use this type of memory to store configuration information.
sesystemprofileprivilege	oval-sc:EntityItemBoolType	0..1	false	Gives the user the privilege to profile system performance.
sesystemtimeprivilege	oval-sc:EntityItemBoolType	0..1	false	Gives the user the privilege to change the system time.
setakeownershipprivilege	oval-sc:EntityItemBoolType	0..1	false	Gives the user the privilege to take ownership of files or other objects. It allows the owner value to be set **only** to those values that the holder may legitimately assign as the owner of an object.
setcbprivilege	oval-sc:EntityItemBoolType	0..1	false	Gives the user the privilege to

				act as part of the operating system, i.e. as part of the Trusted Computer Base (TCB). Some trusted protected subsystems are granted this privilege.
setimezoneprivilege	oval-sc:EntityItemBoolType	0..1	false	Gives the user the privilege to change the time zone.
seundockprivilege	oval-sc:EntityItemBoolType	0..1	false	Gives the user the privilege to remove the computer from a docking station.
seunsolicitedinputprivilege	oval-sc:EntityItemBoolType	0..1	false	Allows the user to read unsolicited input from a terminal device.
sebatchlogonright	oval-sc:EntityItemBoolType	0..1	false	Grants the right for an account to log on using the batch logon type.
seinteractivelogonright	oval-sc:EntityItemBoolType	0..1	false	Grants the right for an account to log on using the interactive logon type.
senetworklogonright	oval-sc:EntityItemBoolType	0..1	false	Grants the right for an account to log on using the network logon type.
seremoteinteractivelogonright	oval-sc:EntityItemBoolType	0..1	false	Grants the right for an account to log on remotely using the interactive logon type.
seservicelogonright	oval-sc:EntityItemBoolType	0..1	false	Grants the right for an account to log on using the service logon type.
sedenybatchLogonright	oval-sc:EntityItemBoolType	0..1	false	Denies the right for an account to log on using the batch logon type.
sedenyinteractivelogonright	oval-sc:EntityItemBoolType	0..1	false	Denies the right for an account to log on using the interactive logon type.
sedenynetworklogonright	oval-sc:EntityItemBoolType	0..1	false	Denies the right for an account to log on using the network logon type.
sedenyremoteInteractivelogonright	oval-sc:EntityItemBoolType	0..1	false	Denies the right for an account to log on remotely using the interactive logon type.
sedenyservicelogonright	oval-sc:EntityItemBoolType	0..1	false	Denies the right for an account to log on using the service logon type.

setrustedcredmanaccessnameright	oval-sc:EntityItemBoolType	0..1	false	Gives the user the privilege to access Credential Manager as a trusted caller. NOTE: This is a privilege (referred to as SE_TRUSTED_CREDMAN_ACCESS_NAME), not a right.

2.39. win-def:auditeventpolicy_test

The `auditeventpolicy_test` is used to make assertions about the different types of events the system should audit[195]. The `auditeventpolicy_test` MUST reference one `auditeventpolicy_object` and zero or more `auditeventpolicy_states`.


oval-def::oval-def::TestType
-id : TestIDPattern
-version : unsigned int
-check_existence : ExistenceEnumeration = at_least_one_exists
-check : CheckEnumeration
-state_operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::auditeventpolicy_test
win-def::auditeventpolicy_state
win-def::auditeventpolicy_object

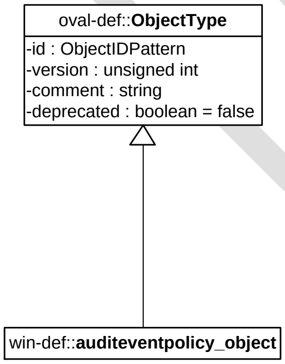
2.39.1. Known Supported Platforms

Comment [DJH5]: We probably want to consider adding windows 2000, windows server 2003, windows server 2008, and windows server 2008 r2.

- Windows XP
- Windows Vista
- Windows 7

2.40. win-def:auditeventpolicy_object

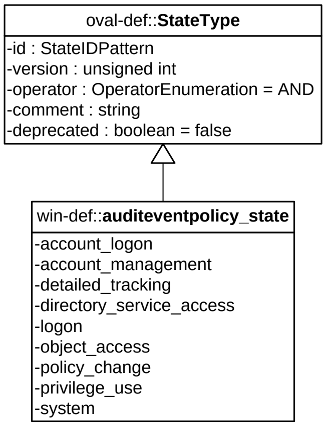
The `auditeventpolicy_object` construct defines the set of audit events whose associated information should be collected and represented as `auditeventpolicy_items`. Because there is only one object relating to audit event policy (the system as a whole), there are no child entities defined for this object,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



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

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	Nillable	Description
account_logon	win-def: EntityStateAuditType	0..1	false	The OS MUST audit each instance of a user attempt to log on or log off this computer, as well as audit logon attempts by privileged accounts that log on to the domain controller.
account_management	win-def: EntityStateAuditType	0..1	false	The OS MUST audit attempts to create, delete, or change user or group accounts, as well as perform password changes.
detailed_tracking	win-def: EntityStateAuditType	0..1	false	The OS MUST audit specific events, such as program activation, some forms of handle duplication, indirect access to an object, and process exit.
directory_service_a	win-def:	0..1	false	The OS MUST audit attempts

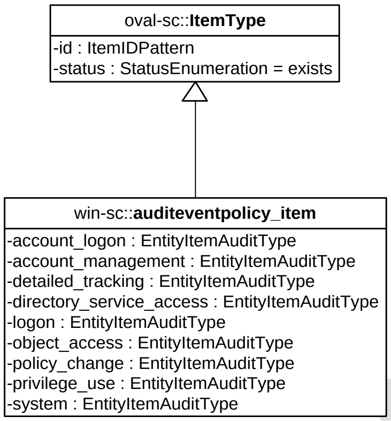
[196] For more information see http://msdn.microsoft.com/en-us/library/windows/desktop/ms721903(v=vs.85).aspx

ccess	EntityStateAuditType			to access the directory service.
logon	win-def:EntityStateAuditType	0..1	false	The OS MUST audit each time this computer validates the credentials of an account.
object_access	win-def: EntityStateAuditType	0..1	false	The OS MUST audit each instance of user attempts to access a non-Active Directory object, such as a file, that has its own system access control (SACL) specified. The type of access request, such as Write, Read, or Modify, and the account making the request MUST match the settings in the SACL.
policy_change	win-def: EntityStateAuditType	0..1	false	The OS must audit attempts to change Policy object rules, such as user rights assignment policy, audit policy, account policy, or trust policy.
privilege_use	win-def: EntityStateAuditType	0..1	false	The OS must audit each instance of user attempts to use privileges.
system	win-def: EntityStateAuditType	0..1	false	The OS must audit attempts to change the system time, startup, restart, or shutdown the system, and load extensible authentication features. Also, it should audit the loss of audited events due to auditing system failure and any instance of a security log size that exceeds a configurable warning threshold level.

Comment [MS6]: Is this actually being checked or monitored in the Windows schema?

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].


oval-sc::ItemType
-id : ItemIDPattern
-status : StatusEnumeration = exists
win-sc::auditeventpolicy_item
-account_logon : EntityItemAuditType
-account_management : EntityItemAuditType
-detailed_tracking : EntityItemAuditType
-directory_service_access : EntityItemAuditType
-logon : EntityItemAuditType
-object_access : EntityItemAuditType
-policy_change : EntityItemAuditType
-privilege_use : EntityItemAuditType
-system : EntityItemAuditType

Property	Type	Multiplicity	Nillable	Description
account_logon	win-def: EntityItemAuditType	0..1	false	The OS MUST audit each instance of a user attempt to log on or log off this computer, as well as audit logon attempts by privileged accounts that log on to the domain controller.
account_management	win-def: EntityItemAuditType	0..1	false	The OS MUST audit attempts to create, delete, or change user or group accounts, as well as perform password changes.
detailed_tracking	win-def: EntityItemAuditType	0..1	false	The OS MUST audit specific events, such as program activation, some forms of handle duplication, indirect access to an object, and process exit.
directory_service_access	win-def: EntityItemAuditType	0..1	false	The OS MUST audit attempts to access the directory

[197] For more information see 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.

Comment [MS7]: Is this actually being checked or monitored in the Windows schema?

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.

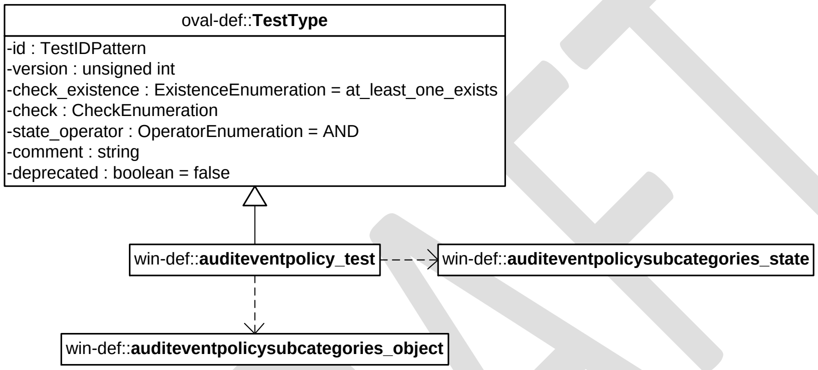
2.44. win-sc:EntityItemAuditType

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 system[198]. The `auditeventpolicysubcategories_test` MUST reference one `auditeventpolicysubcategories_object` and zero or more `auditeventpolicysubcategories_states`.


oval-def::**TestType**
-id : TestIDPattern
-version : unsigned int
-check_existence : ExistenceEnumeration = at_least_one_exists
-check : CheckEnumeration
-state_operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::**auditeventpolicy_test**
win-def::**auditeventpolicysubcategories_state**
win-def::**auditeventpolicysubcategories_object**

2.45.1. Known Supported Platforms

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

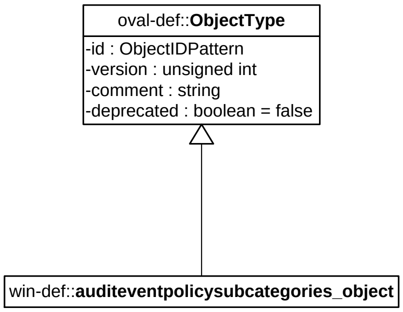
Comment [DJH8]: We probably want to consider adding windows 2000, windows server 2003, windows server 2008, and windows server 2008 r2.

Comment [MS9]: The Kerberos Ticket Event category is not listed on the MSDN website.

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.

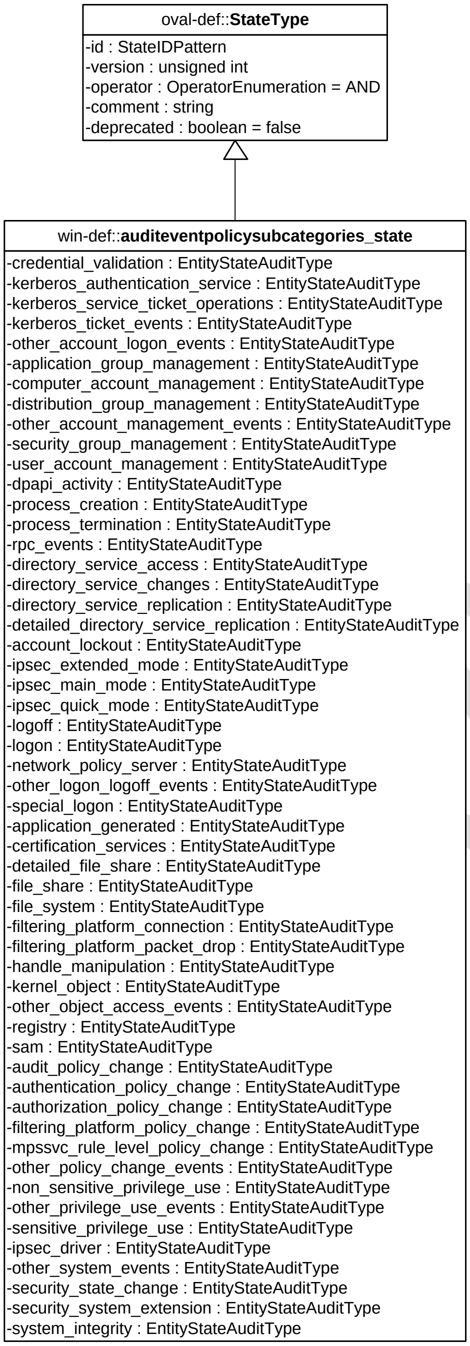
[198] For more information see http://msdn.microsoft.com/en-us/library/dd976913(v=PROT.10).aspx



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 platforms[199].

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


oval-def::**StateType**
-id : StateIDPattern
-version : unsigned int
-operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::**auditeventpolicysubcategories_state**
-credential_validation : EntityStateAuditType
-kerberos_authentication_service : EntityStateAuditType
-kerberos_service_ticket_operations : EntityStateAuditType
-kerberos_ticket_events : EntityStateAuditType
-other_account_logon_events : EntityStateAuditType
-application_group_management : EntityStateAuditType
-computer_account_management : EntityStateAuditType
-distribution_group_management : EntityStateAuditType
-other_account_management_events : EntityStateAuditType
-security_group_management : EntityStateAuditType
-user_account_management : EntityStateAuditType
-dpapi_activity : EntityStateAuditType
-process_creation : EntityStateAuditType
-process_termination : EntityStateAuditType
-rpc_events : EntityStateAuditType
-directory_service_access : EntityStateAuditType
-directory_service_changes : EntityStateAuditType
-directory_service_replication : EntityStateAuditType
-detailed_directory_service_replication : EntityStateAuditType
-account_lockout : EntityStateAuditType
-ipsec_extended_mode : EntityStateAuditType
-ipsec_main_mode : EntityStateAuditType
-ipsec_quick_mode : EntityStateAuditType
-logoff : EntityStateAuditType
-logon : EntityStateAuditType
-network_policy_server : EntityStateAuditType
-other_logon_logoff_events : EntityStateAuditType
-special_logon : EntityStateAuditType
-application_generated : EntityStateAuditType
-certification_services : EntityStateAuditType
-detailed_file_share : EntityStateAuditType
-file_share : EntityStateAuditType
-file_system : EntityStateAuditType
-filtering_platform_connection : EntityStateAuditType
-filtering_platform_packet_drop : EntityStateAuditType
-handle_manipulation : EntityStateAuditType
-kernel_object : EntityStateAuditType
-other_object_access_events : EntityStateAuditType
-registry : EntityStateAuditType
-sam : EntityStateAuditType
-audit_policy_change : EntityStateAuditType
-authentication_policy_change : EntityStateAuditType
-authorization_policy_change : EntityStateAuditType
-filtering_platform_policy_change : EntityStateAuditType
-mpssvc_rule_level_policy_change : EntityStateAuditType
-other_policy_change_events : EntityStateAuditType
-non_sensitive_privilege_use : EntityStateAuditType
-other_privilege_use_events : EntityStateAuditType
-sensitive_privilege_use : EntityStateAuditType
-ipsec_driver : EntityStateAuditType
-other_system_events : EntityStateAuditType
-security_state_change : EntityStateAuditType
-security_system_extension : EntityStateAuditType
-system_integrity : EntityStateAuditType

Property	Type	Multiplicity	Nillable	Description
credential_validation	win-def: EntityStateAuditType	0..1	false	The OS MUST audit events that are generated by validation tests on user account logon credentials. This has GUID {0CCE923F-69AE-11D9-BED3-505054503030}.
kerberos_authentication_service	win-def: EntityStateAuditType	0..1	false	The OS MUST audit events that are generated by Kerberos authentication ticket-granting ticket (TGT) requests. This has GUID {0CCE9242-69AE-11D9-BED3-505054503030}.
kerberos_service_ticket_operations	win-def: EntityStateAuditType	0..1	false	The OS MUST audit events that are generated by Kerberos service ticket requests. This has GUID {0CCE9240-69AE-11D9-BED3-505054503030}.
kerberos_ticket_events	win-def: EntityStateAuditType	0..1	false	The OS MUST audit events that involve validation tests on Kerberos tickets submitted for a user account logon request.[200]
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

Comment [MS10]: Is there a reference that says what the GUID is it?

[200] For more information see 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: 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/0e57a2df-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	The OS must audit events generated when a handle to an object is opened or closed. Only objects with a matching SACL generate security audit events. Open and close handle events will be audited when both the Handle Manipulation subcategory is enabled along with the corresponding resource manager identified by other Object Access audit subcategory, like File System or Registry. Enabling Handle Manipulation causes implementation-specific security event data to be logged identifying the permissions that were used to grant or deny the access

				requested by the user; this is also known as "Reason for access". This has GUID {0CCE9223-69AE-11D9-BED3-505054503030}.
kernel_object	win-def: EntityStateAuditType	0..1	false	The OS must audit attempts to access the system kernel, which include mutexes and semaphores. Only kernel objects with a matching SACL generate security audit events. This has GUID {0CCE921F-69AE-11D9-BED3-505054503030}.
other_object_access_events	win-def: EntityStateAuditType	0..1	false	The OS must audit events generated by the management of Task Scheduler jobs or COM+ objects.
registry	win-def: EntityStateAuditType	0..1	false	The OS must audit attempts to access registry objects. A security audit event is generated only for objects that have SACLs and only if the type of access requested, such as Read, Write, or Modify, and the account making the request match the settings in the SACL. This has GUID {0CCE921E-69AE-11D9-BED3-505054503030}.
sam	win-def: EntityStateAuditType	0..1	false	The OS must audit events generated by attempts to access Security Accounts Manager (SAM) objects. This has GUID {0CCE9220-69AE-11D9-BED3-505054503030}.
audit_policy_change	win-def: EntityStateAuditType	0..1	false	The OS must audit changes in security audit policy settings. This has GUID {0CCE922F-69AE-11D9-BED3-505054503030}.
authentication_policy_change	win-def: EntityStateAuditType	0..1	false	The OS must audit events generated by changes to the authentication policy. This has GUID {0CCE9230-69AE-

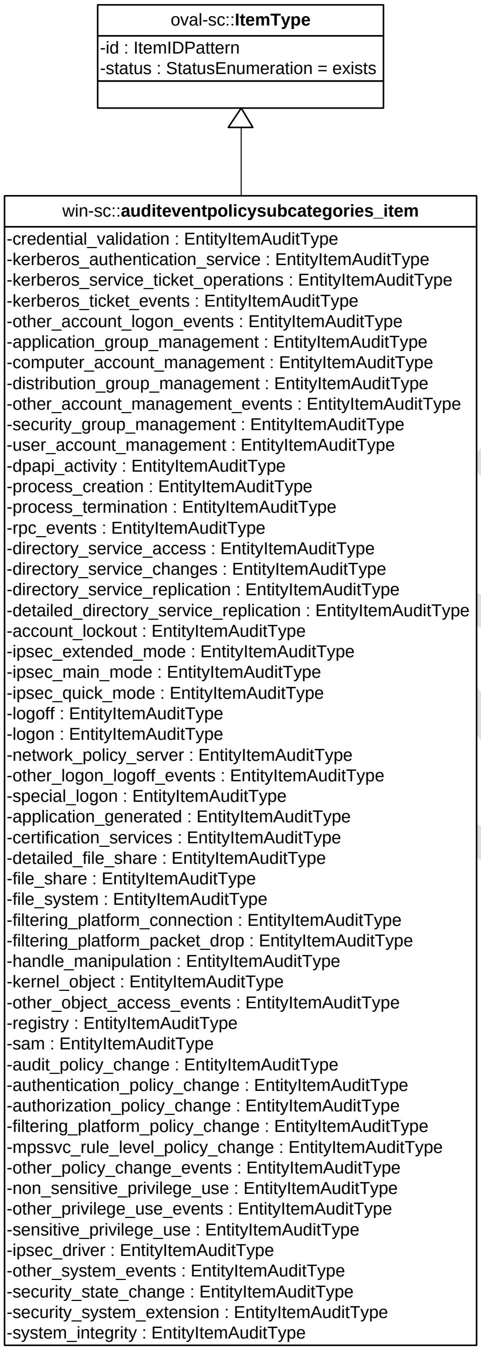
				11D9-BED3-505054503030}.
authorization_policy_change	win-def: EntityStateAuditType	0..1	false	The OS must audit events generated by changes to the authorization policy. This has GUID {0CCE9231-69AE-11D9-BED3-505054503030}.
filtering_platform_policy_change	win-def: EntityStateAuditType	0..1	false	The OS must audit events generated by changes to the Windows Filtering Platform (WFP). This has GUID {0CCE9233-69AE-11D9-BED3-505054503030}.
mpssvc_rule_level_policy_change	win-def: EntityStateAuditType	0..1	false	The OS must audit events generated by changes in policy rules used by Windows Firewall. This has GUID {0CCE9232-69AE-11D9-BED3-505054503030}.
other_policy_change_events	win-def: EntityStateAuditType	0..1	false	The OS must audit events generated by other security policy changes that are not audited in the Policy Change category. This has GUID {0CCE9234-69AE-11D9-BED3-505054503030}.
non_sensitive_privilege_use	win-def: EntityStateAuditType	0..1	false	The OS must audit events generated by the use of nonsensitive privileges (user rights), such as logging on locally or with a Remote Desktop connection, changing the system time, or removing a computer from a docking station. This has GUID {0CCE9229-69AE-11D9-BED3-505054503030}.
other_privilege_use_events	win-def: EntityStateAuditType	0..1	false	The OS must TODO. This has GUID {0CCE922A-69AE-11D9-BED3-505054503030}.
sensitive_privilege_use	win-def: EntityStateAuditType	0..1	false	The OS must audit events generated by the use of sensitive privileges (user rights), such as acting as part of the operating system, backing up files and directories, impersonating a client computer, or

				generating security audits. This has GUID {0CCE9228-69AE-11D9-BED3-505054503030}.
ipsec_driver	win-def: EntityStateAuditType	0..1	false	The OS must audit events that are generated by the IPsec filter driver. This has GUID {0CCE9213-69AE-11D9-BED3-505054503030}.
other_system_events	win-def: EntityStateAuditType	0..1	false	The OS must audit any of the following events: - Startup and shutdown of the Windows Firewall. - Security policy processing by the Windows Firewall. - Cryptography key file and migration operations. This has GUID {0CCE9214-69AE-11D9-BED3-505054503030}.
security_state_change	win-def: EntityStateAuditType	0..1	false	The OS must audit events generated by changes in the security state of the computer. This has GUID {0CCE9210-69AE-11D9-BED3-505054503030}.
security_system_extension	win-def: EntityStateAuditType	0..1	false	The OS must audit events related to security system extensions or services. This has GUID {0CCE9211-69AE-11D9-BED3-505054503030}.
system_integrity	win-def: EntityStateAuditType	0..1	false	The OS must audit events that violate the integrity of the security subsystem. This has GUID {0CCE9212-69AE-11D9-BED3-505054503030}.

2.48. win-sc:auditeventpolicysubcategories_item

The `auditeventpolicysubcategories_item` construct stores the different subcategories of event types the system should audit[202].

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


oval-sc::**ItemType**
-id : ItemIDPattern
-status : StatusEnumeration = exists
win-sc::**auditeventpolicysubcategories_item**
-credential_validation : EntityItemAuditType
-kerberos_authentication_service : EntityItemAuditType
-kerberos_service_ticket_operations : EntityItemAuditType
-kerberos_ticket_events : EntityItemAuditType
-other_account_logon_events : EntityItemAuditType
-application_group_management : EntityItemAuditType
-computer_account_management : EntityItemAuditType
-distribution_group_management : EntityItemAuditType
-other_account_management_events : EntityItemAuditType
-security_group_management : EntityItemAuditType
-user_account_management : EntityItemAuditType
-dpapi_activity : EntityItemAuditType
-process_creation : EntityItemAuditType
-process_termination : EntityItemAuditType
-rpc_events : EntityItemAuditType
-directory_service_access : EntityItemAuditType
-directory_service_changes : EntityItemAuditType
-directory_service_replication : EntityItemAuditType
-detailed_directory_service_replication : EntityItemAuditType
-account_lockout : EntityItemAuditType
-ipsec_extended_mode : EntityItemAuditType
-ipsec_main_mode : EntityItemAuditType
-ipsec_quick_mode : EntityItemAuditType
-logoff : EntityItemAuditType
-logon : EntityItemAuditType
-network_policy_server : EntityItemAuditType
-other_logon_logoff_events : EntityItemAuditType
-special_logon : EntityItemAuditType
-application_generated : EntityItemAuditType
-certification_services : EntityItemAuditType
-detailed_file_share : EntityItemAuditType
-file_share : EntityItemAuditType
-file_system : EntityItemAuditType
-filtering_platform_connection : EntityItemAuditType
-filtering_platform_packet_drop : EntityItemAuditType
-handle_manipulation : EntityItemAuditType
-kernel_object : EntityItemAuditType
-other_object_access_events : EntityItemAuditType
-registry : EntityItemAuditType
-sam : EntityItemAuditType
-audit_policy_change : EntityItemAuditType
-authentication_policy_change : EntityItemAuditType
-authorization_policy_change : EntityItemAuditType
-filtering_platform_policy_change : EntityItemAuditType
-mpssvc_rule_level_policy_change : EntityItemAuditType
-other_policy_change_events : EntityItemAuditType
-non_sensitive_privilege_use : EntityItemAuditType
-other_privilege_use_events : EntityItemAuditType
-sensitive_privilege_use : EntityItemAuditType
-ipsec_driver : EntityItemAuditType
-other_system_events : EntityItemAuditType
-security_state_change : EntityItemAuditType
-security_system_extension : EntityItemAuditType
-system_integrity : EntityItemAuditType

Property	Type	Multiplicity	Nillable	Description
credential_validation	win-def:EntityItemAuditType	0..1	false	The OS MUST audit events that are generated by validation tests on user account logon credentials. This has GUID {0CCE923F-69AE-11D9-BED3-505054503030}.
kerberos_authentication_service	win-def:EntityItemAuditType	0..1	false	The OS MUST audit events that are generated by Kerberos authentication ticket-granting ticket (TGT) requests. This has GUID {0CCE9242-69AE-11D9-BED3-505054503030}.
kerberos_service_ticket_operations	win-def:EntityItemAuditType	0..1	false	The OS MUST audit events that are generated by Kerberos service ticket requests. This has GUID {0CCE9240-69AE-11D9-BED3-505054503030}.
kerberos_ticket_events	win-def:EntityItemAuditType	0..1	false	The OS MUST audit events that involve validation tests on Kerberos tickets submitted for a user account logon request.[203]
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

Comment [MS11]: Is there a reference that says this GUID is?

[203] For more information see 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

				{0CCE9217-69AE-11D9-BED3-505054503030}.
ipsec_extended_mode	win-def:EntityItemAuditType	0..1	false	The OS must audit events generated by Internet Key Exchange protocol (IKE) and Authenticated Internet Protocol (AuthIP) during Extended Mode negotiations. This has GUID {0CCE921A-69AE-11D9-BED3-505054503030}.
ipsec_main_mode	win-def:EntityItemAuditType	0..1	false	The OS must audit events generated by Internet Key Exchange protocol (IKE) and Authenticated Internet Protocol (AuthIP) during Main Mode negotiations. This has GUID {0CCE9218-69AE-11D9-BED3-505054503030}.
ipsec_quick_mode	win-def:EntityItemAuditType	0..1	false	The OS must audit events generated by Internet Key Exchange protocol (IKE) and Authenticated Internet Protocol (AuthIP) during Quick Mode negotiations. This has GUID {0CCE9219-69AE-11D9-BED3-505054503030}.
logoff	win-def:EntityItemAuditType	0..1	false	The OS must audit events generated by closing a logon session. These events occur on the computer that was accessed. For an interactive logon, the security audit event is generated on the computer that the user account logged on to. This has GUID {0CCE9216-69AE-11D9-BED3-505054503030}.
logon	win-def:EntityItemAuditType	0..1	false	The OS must audit events generated by user account logon attempts on a computer. This has GUID {0CCE9215-69AE-11D9-BED3-505054503030}.
network_policy_server	win-def:EntityItemAuditType	0..1	false	The OS must audit events generated by RADIUS (IAS)

				and Network Access Protection (NAP) user access requests. These requests can be Grant, Deny, Discard, Quarantine, Lock, and Unlock. This has GUID {0CCE9243-69AE-11D9-BED3-505054503030}.
other_logon_logoff_events	win-def:EntityItemAuditType	0..1	false	The OS must audit events generated by other events related to logon and logoff that are not included in the Logon/Logoff category. This has GUID {0CCE921C-69AE-11D9-BED3-505054503030}.
special_logon	win-def:EntityItemAuditType	0..1	false	The OS must audit events generated by special logons. This has GUID {0CCE921B-69AE-11D9-BED3-505054503030}.
application_generated	win-def:EntityItemAuditType	0..1	false	The OS must audit applications that generate events by using the Windows Auditing application programming interfaces (APIs). Applications designed to use the Windows Auditing API use this subcategory to log auditing events related to their function. This has GUID {0CCE9222-69AE-11D9-BED3-505054503030}.
certification_services	win-def:EntityItemAuditType	0..1	false	The OS must audit Active Directory Certificate Services (AD CS) operations. This has GUID {0CCE9221-69AE-11D9-BED3-505054503030}.
detailed_file_share	win-def:EntityItemAuditType	0..1	false	The OS must audit every attempt to access objects in a shared folder. This has GUID {0CCE9244-69AE-11D9-BED3-505054503030}.
file_share	win-def:EntityItemAuditType	0..1	false	The OS must audit attempts to access a shared folder. This has GUID {0CCE9224-69AE-

				11D9-BED3-505054503030}.
file_system	win-def:EntityItemAuditType	0..1	false	The OS must audit attempts to access file system objects. A security audit event is generated only for objects that have SACLs and only if the type of access requested, such as Write, Read, or Modify, and the account making the request match the settings in the SACL. This has GUID {0CCE921D-69AE-11D9-BED3-505054503030}.
filtering_platform_connection	win-def:EntityItemAuditType	0..1	false	The OS must audit connections that are allowed or blocked by the Windows Filtering Platform (WFP). This has GUID {0CCE9226-69AE-11D9-BED3-505054503030}.
filtering_platform_packet_drop	win-def:EntityItemAuditType	0..1	false	This OS must audit packets that are dropped by the Windows Filtering Platform (WFP).
handle_manipulation	win-def:EntityItemAuditType	0..1	false	The OS must audit events generated when a handle to an object is opened or closed. Only objects with a matching SACL generate security audit events. Open and close handle events will be audited when both the Handle Manipulation subcategory is enabled along with the corresponding resource manager identified by other Object Access audit subcategory, like File System or Registry. Enabling Handle Manipulation causes implementation-specific security event data to be logged identifying the permissions that were used

				to grant or deny the access requested by the user; this is also known as "Reason for access". This has GUID {0CCE9223-69AE-11D9-BED3-505054503030}.
kernel_object	win-def:EntityItemAuditType	0..1	false	The OS must audit attempts to access the system kernel, which include mutexes and semaphores. Only kernel objects with a matching SACL generate security audit events. This has GUID {0CCE921F-69AE-11D9-BED3-505054503030}.
other_object_access_events	win-def:EntityItemAuditType	0..1	false	The OS must audit events generated by the management of Task Scheduler jobs or COM+ objects.
registry	win-def:EntityItemAuditType	0..1	false	The OS must audit attempts to access registry objects. A security audit event is generated only for objects that have SACLs and only if the type of access requested, such as Read, Write, or Modify, and the account making the request match the settings in the SACL. This has GUID {0CCE921E-69AE-11D9-BED3-505054503030}.
sam	win-def:EntityItemAuditType	0..1	false	The OS must audit events generated by attempts to access Security Accounts Manager (SAM) objects. This has GUID {0CCE9220-69AE-11D9-BED3-505054503030}.
audit_policy_change	win-def:EntityItemAuditType	0..1	false	The OS must audit changes in security audit policy settings. This has GUID {0CCE922F-69AE-11D9-BED3-505054503030}.
authentication_policy_change	win-def:EntityItemAuditType	0..1	false	The OS must audit events generated by changes to the authentication policy. This

				has GUID {0CCE9230-69AE-11D9-BED3-505054503030}.
authorization_policy_change	win-def:EntityItemAuditType	0..1	false	The OS must audit events generated by changes to the authorization policy. This has GUID {0CCE9231-69AE-11D9-BED3-505054503030}.
filtering_platform_policy_change	win-def:EntityItemAuditType	0..1	false	The OS must audit events generated by changes to the Windows Filtering Platform (WFP). This has GUID {0CCE9233-69AE-11D9-BED3-505054503030}.
mpssvc_rule_level_policy_change	win-def:EntityItemAuditType	0..1	false	The OS must audit events generated by changes in policy rules used by Windows Firewall. This has GUID {0CCE9232-69AE-11D9-BED3-505054503030}.
other_policy_change_events	win-def:EntityItemAuditType	0..1	false	The OS must audit events generated by other security policy changes that are not audited in the Policy Change category. This has GUID {0CCE9234-69AE-11D9-BED3-505054503030}.
non_sensitive_privilege_use	win-def:EntityItemAuditType	0..1	false	The OS must audit events generated by the use of nonsensitive privileges (user rights), such as logging on locally or with a Remote Desktop connection, changing the system time, or removing a computer from a docking station. This has GUID {0CCE9229-69AE-11D9-BED3-505054503030}.
other_privilege_use_events	win-def:EntityItemAuditType	0..1	false	Not used. This has GUID {0CCE922A-69AE-11D9-BED3-505054503030}.
sensitive_privilege_use	win-def:EntityItemAuditType	0..1	false	The OS must audit events generated by the use of sensitive privileges (user rights), such as acting as part of the operating system, backing up files and directories, impersonating a

				client computer, or generating security audits. This has GUID {0CCE9228-69AE-11D9-BED3-505054503030}.
ipsec_driver	win-def:EntityItemAuditType	0..1	false	The OS must audit events that are generated by the IPsec filter driver. This has GUID {0CCE9213-69AE-11D9-BED3-505054503030}.
other_system_events	win-def:EntityItemAuditType	0..1	false	The OS must audit any of the following events: - Startup and shutdown of the Windows Firewall. - Security policy processing by the Windows Firewall. - Cryptography key file and migration operations. This has GUID {0CCE9214-69AE-11D9-BED3-505054503030}.
security_state_change	win-def:EntityItemAuditType	0..1	false	The OS must audit events generated by changes in the security state of the computer. This has GUID {0CCE9210-69AE-11D9-BED3-505054503030}.
security_system_extension	win-def:EntityItemAuditType	0..1	false	The OS must audit events related to security system extensions or services. This has GUID {0CCE9211-69AE-11D9-BED3-505054503030}.
system_integrity	win-def:EntityItemAuditType	0..1	false	The OS must audit events that violate the integrity of the security subsystem. This has GUID {0CCE9212-69AE-11D9-BED3-505054503030}.

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.

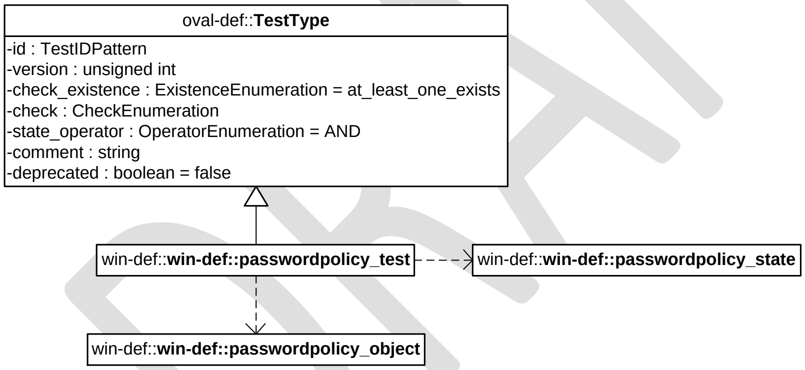
2.50. win-sc:EntityItemAuditType

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 systems[205]. It is important to note that these policies are specific to certain versions of Windows. Additionally, this information is stored in the SAM or Active Directory and is **encrypted or hidden**, thus the registry_test and activedirectory57_test are of NO USE. The passwordpolicy_test MUST reference one passwordpolicy_object and zero or more passwordpolicy_states.


oval-def::**TestType**
-id : TestIDPattern
-version : unsigned int
-check_existence : ExistenceEnumeration = at_least_one_exists
-check : CheckEnumeration
-state_operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::**win-def::passwordpolicy_test**
win-def::**win-def::passwordpolicy_state**
win-def::**win-def::passwordpolicy_object**

2.51.1. Known Supported Platforms

Comment [DJH12]: We probably want to consider adding windows 2000, windows server 2003, windows server 2008, and windows server 2008 r2.

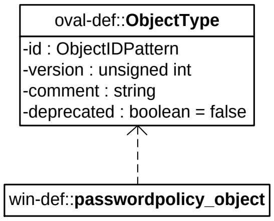
- Windows XP
- Windows Vista
- Windows 7

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

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.

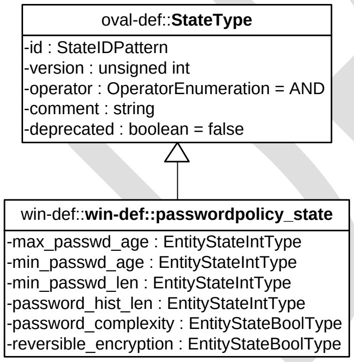


2.53. win-def:passwordpolicy_state

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 platforms[206].

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

Comment [DJH13]: This is found in Microsoft's lmaccess.h . Maybe we can find a Microsoft link for this.


oval-def::**StateType**
-id : StateIDPattern
-version : unsigned int
-operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::**win-def::passwordpolicy_state**
-max_passwd_age : EntityStateIntType
-min_passwd_age : EntityStateIntType
-min_passwd_len : EntityStateIntType
-password_hist_len : EntityStateIntType
-password_complexity : EntityStateBoolType
-reversible_encryption : EntityStateBoolType

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

[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

				password can be used before the system requires the user to change it. In OVAL, values range from 1 * 86400 (one day) to 999 * 86400 = 86313600 (999 days) inclusive, where 86400 is the number of seconds in one day. In addition, max_passwd_age can take on the value of TIMEQ_FOREVER to indicate that passwords NEVER expire. The default in the Default Domain Group Policy Object (GPO), as well as workstations and servers, is 42*86400 = 3628800 (42 days).
min_passwd_age	oval-def:EntityStateIntType	0..1	false	Alternate name: "Minimum password age." Determines the period (in seconds) that a password must be used before the user can change it. In OVAL, values range from 0 * 86400 (changes can happen immediately) to 999 * 86400 = 86313600 (999 days) inclusive, where 86400 is the number of seconds in one day. The default in the Default Domain GPO, as well as workstations and servers, is 0.
min_passwd_len	oval-def:EntityStateIntType	0..1	false	Alternate name: "Minimum password length." Determines the least number of characters a user account's password may contain. In OVAL, values range from 0 to 14 inclusive, where 0 indicates that no password is

				required. The default in the Default Domain GPO, as well as workstations and servers, is 0.
password_hist_len	oval-def:EntityStateIntType	0..1	false	Alternate name: "Enforce password history." Determines the number of unique new passwords that have to be associated with a user account before an old password can be reused. Values range from 0 to 24 inclusive. The default in the Default Domain GPO, as well as workstations and servers, is 1.
password_complexity	oval-def: EntityStateBoolType	0..1	false	Alternate name: "Password must meet complexity requirements (of the installed password filter)." The part in parenthesis is different depending on the version of Windows in question. This attribute determines whether passwords meet complexity requirements. The default password filter defined by passfilt.dll (found in Win 2000, but also applies in later versions) requires that a password 1) does not contain all or part of the user's account name, 2) is at least six characters in length, and 3) satisfies three out of the four criteria of containing either uppercase, lowercase, base 10 digits 0-9, and/or nonalphanumeric characters. Complexity requirements are enforced upon password change or creation. The default in the Default Domain GPO, as well as workstations and servers, is "Disabled," or

				0 in OVAL.
reversible_encryption	oval-def: EntityStateBoolType	0..1	false	Alternate name: "Store password using reversible encryption (for all users in the domain)." The part in parenthesis is different depending on the version of Windows in question. This determines whether Windows will store passwords using reversible encryption. According to MSDN, storing passwords using reversible encryption is essentially the same as storing clear-text versions of the passwords, so it SHOULD NEVER BE ENABLED unless application requirements outweigh the need to protect password information. The default in the Default Domain GPO, as well as workstations and servers, is "Disabled," or 0 in OVAL.

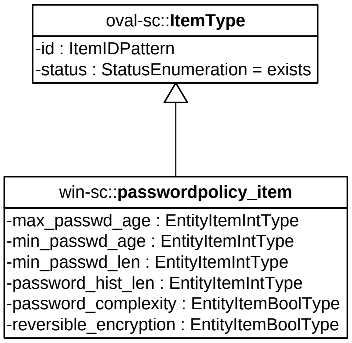
2.54. win-sc:passwordpolicy_item

The `passwordpolicy_item` construct stores the different policies on password that should be collected[208].

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

[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


oval-sc::ItemType
-id : ItemIDPattern
-status : StatusEnumeration = exists
win-sc::passwordpolicy_item
-max_passwd_age : EntityItemIntType
-min_passwd_age : EntityItemIntType
-min_passwd_len : EntityItemIntType
-password_hist_len : EntityItemIntType
-password_complexity : EntityItemBoolType
-reversible_encryption : EntityItemBoolType

Property	Type	Multiplicity	Nillable	Description
max_passwd_age	oval-def:EntityItemIntType	0..1	false	Alternate name: "Maximum password age." Determines the period (in seconds) that a password can be used before the system requires the user to change it. In OVAL, values range from 1 * 86400 (one day) to 999 * 86400 = 86313600 (999 days) inclusive, where 86400 is the number of seconds in one day. In addition, max_passwd_age can take on the value of TIMEQ_FOREVER to indicate that passwords NEVER expire. The default in the Default Domain Group Policy Object (GPO), as well as workstations and servers is 42*86400 = 3628800 (42 days).
min_passwd_age	oval-def:EntityItemIntType	0..1	false	Alternate name: "Minimum password age." Determines the period (in seconds) that a password must be used before the user can change it. In OVAL, values range from 0

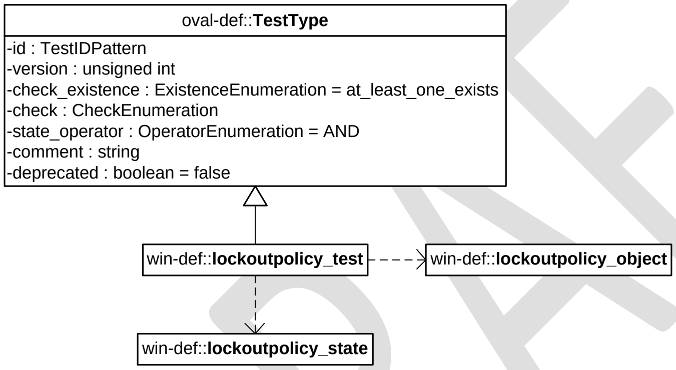
				* 86400 (changes can happen immediately) to 999 * 86400 = 86313600 (999 days) inclusive, where 86400 is the number of seconds in one day. The default in the Default Domain GPO, as well as workstations and servers, is 0.
min_passwd_len	oval-def:EntityItemIntType	0..1	false	Alternate name: "Minimum password length." Determines the least number of characters a user account's password may contain. In OVAL, values range from 0 to 14 inclusive, where 0 indicates that no password is required. The default in the Default Domain GPO, as well as workstations and servers, is 0.
password_hist_len	oval-def:EntityItemIntType	0..1	false	Alternate name: "Enforce password history." Determines the number of unique new passwords that have to be associated with a user account before an old password can be reused. Values range from 0 to 24 inclusive. The default in the Default Domain GPO, as well as workstations and servers, is 1.
password_complexity	oval-def: EntityItemBoolType	0..1	false	Alternate name: "Password must meet complexity requirements (of the installed password filter)." The part in parenthesis is different depending on the version of Windows in question.

				This attribute determines whether passwords meet complexity requirements. The default password filter defined by passfilt.dll (found in Win 2000, but also applies in later versions) requires that a password 1) does not contain all or part of the user's account name, 2) is at least six characters in length, and 3) satisfies three out of the four criteria of containing either uppercase, lowercase, base 10 digits 0-9, and/or nonalphanumeric characters. Complexity requirements are enforced upon password change or creation. The default in the Default Domain GPO, as well as workstations and servers, is "Disabled," or 0 in OVAL.
reversible_encryption	oval-def: EntityItemBoolType	0..1	false	Alternate name: "Store password using reversible encryption (for all users in the domain)." The part in parenthesis is different depending on the version of Windows in question. This determines whether Windows will store passwords using reversible encryption. According to MSDN, storing passwords using reversible encryption is essentially the same as storing clear-text versions of the passwords, so it SHOULD NEVER BE ENABLED unless application requirements outweigh the

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

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 database[210]. The `lockoutpolicy_test` MUST reference one `lockoutpolicy_object` and zero or more `lockoutpolicy_states`.


oval-def::TestType
-id : TestIDPattern
-version : unsigned int
-check_existence : ExistenceEnumeration = at_least_one_exists
-check : CheckEnumeration
-state_operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::lockoutpolicy_test
win-def::lockoutpolicy_object
win-def::lockoutpolicy_state

2.55.1. Known Supported Platforms

Comment [DJH14]: We probably want to consider adding windows 2000, windows server 2003, windows server 2008, and windows server 2008 r2.

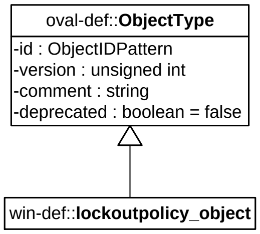
- Windows XP
- Windows Vista
- Windows 7

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
For more information about lockout policies in general see http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=6218

lockoutpolicy_items[211]. Because there is only one object relating to lockout information (the system as a whole), there are no child entities defined for this object, so it is considered empty.



2.57. win-def: lockoutpolicy_state

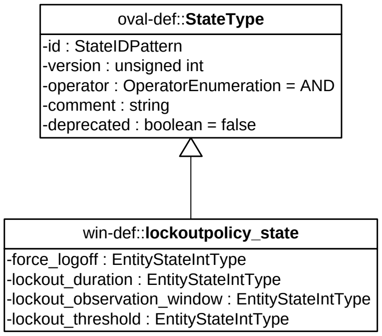
The lockoutpolicy_state construct is used by a lockoutpolicy_test to outline the various attributes associated with lockout information for users and global groups in the security database under Microsoft Windows platforms[212]. In Windows an administrator can go to the Control Panel and go to Local Security Policy. From there, the policies mentioned are under Account Policies/Account Lockout Policy. When mentioning alternate names for specific attributes, they are referring to the ones in that directory path, except for force_logoff and lockout_observation_window[213]. 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
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
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 int[214].


oval-def::StateType
-id : StateIDPattern
-version : unsigned int
-operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::lockoutpolicy_state
-force_logoff : EntityStateIntType
-lockout_duration : EntityStateIntType
-lockout_observation_window : EntityStateIntType
-lockout_threshold : EntityStateIntType

Property	Type	Multiplicity	Nillable	Description
force_logoff	oval-def:EntityStateIntType	0..1	false	Indicates the amount of time in SECONDS (not MINUTES) that an interactive logon session is allowed to continue.
lockout_duration	oval-def:EntityStateIntType	0..1	false	Alternate name: "Account lockout duration." Determines the number of SECONDS a locked-out account remains locked out before automatically becoming unlocked. The available range is from 1 second through 99,999*60 = 5999940 seconds. If an account lockout threshold is defined, the account lockout duration must be greater than or equal to the reset time. If you set the account lockout duration to TIMEQ_FOREVER, the account MUST be locked

Comment [MS15]: Need a reference so I can find out which condition on min and max values this takes on. Also how is this being set by an administrator (not just via command line)?

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

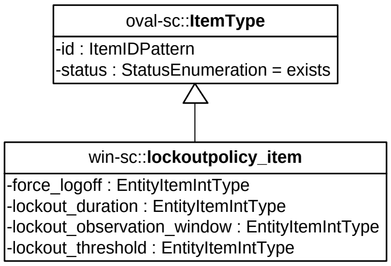
				out until an administrator explicitly unlocks it[215]. This policy on has meaning when Account lockout threshold is specified. The default value is 30 *60 = 1800 (30 minutes).
lockout_observation_window	oval-def:EntityStateIntType	0..1	false	Indicates the amount of time in SECONDS in which failed password attempts are counted without resetting the count to zero. This setting can be used to help mitigate lockout issues that are initiated by users. The available range is from 1 second through 99,999*60 = 5999940 seconds, with a default of 30*60 = 1800 (30 minutes).
lockout_threshold	oval-def:EntityStateIntType	0..1	false	Alternate name: "Account lockout threshold." Determines the number of failed logon attempts that will cause a user account to be locked out. A locked out account cannot be used until it is reset by an administrator or the account lockout duration has expired. You can set values between 1 and 999 failed logon attempts, or you can specify that the account will never be locked out by setting the value to 0. By default, this setting is 0 in the Default Domain Group Policy object (GPO) and in the

[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

				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.


oval-sc::ItemType
-id : ItemIDPattern
-status : StatusEnumeration = exists
win-sc::lockoutpolicy_item
-force_logoff : EntityItemIntType
-lockout_duration : EntityItemIntType
-lockout_observation_window : EntityItemIntType
-lockout_threshold : EntityItemIntType

Property	Type	Multiplicity	Nillable	Description
force_logoff	oval-def:EntityStateIntType	0..1	false	Indicates the amount of time in SECONDS (not MINUTES) that an interactive logon session is allowed to continue.
lockout_duration	oval-def:EntityStateIntType	0..1	false	Alternate name: "Account lockout duration." Determines the number of SECONDS a locked-out account remains locked out before automatically becoming unlocked. The available range is from 1 second through 99,999*60 = 5999940 seconds. If an account lockout threshold is defined, the account lockout duration must be greater than or equal to the reset time. If you set the account lockout duration to TIMEQ_FOREVER, the account MUST be locked out until an administrator

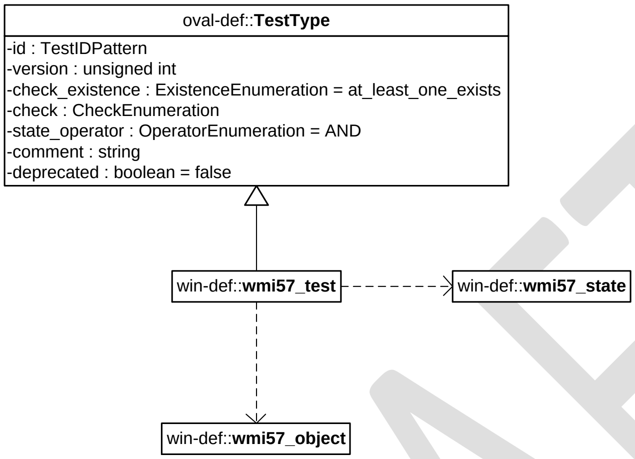
Comment [MS16]: Need a reference so I can find out which condition on min and max values this takes on. Also how is this being set by an administrator (not just via command line)?

				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	Indicates the amount of time in SECONDS in which failed password attempts are counted without resetting the count to zero. This setting can be used to help mitigate lockout issues that are initiated by users. The available range is from 1 second through 99,999*60 = 5999940 seconds, with a default of 30*60 = 1800 (30 minutes).
lockout_threshold	oval-def:EntityStateIntType	0..1	false	Alternate name: "Account lockout threshold." Determines the number of failed logon attempts that will cause a user account to be locked out. A locked out account cannot be used until it is reset by an administrator or the account lockout duration has expired. You can set values between 1 and 999 failed logon attempts, or you can specify that the account will never be locked out by setting the value to 0. By default, this setting is 0 in the Default Domain Group Policy object (GPO) and in the local security policy of workstations and servers.

[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

2.59. win-def:wmi57_test

The `wmi57_test` is used to make assertions about information accessed by WMI[217]. The `wmi57_test` MUST reference one `wmi57_object` and zero or more `wmi57_states`.


oval-def::**TestType**
-id : TestIDPattern
-version : unsigned int
-check_existence : ExistenceEnumeration = at_least_one_exists
-check : CheckEnumeration
-state_operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::**wmi57_test**
win-def::**wmi57_state**
win-def::**wmi57_object**

2.59.1. Known Supported Platforms

Comment [DJH17]: We probably want to consider adding windows 2000, windows server 2003, windows server 2008, and windows server 2008 r2.

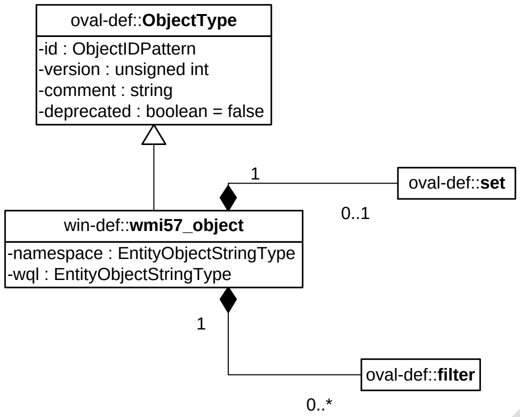
- Windows XP
- Windows Vista
- Windows 7

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	Nillable	Description
set	oval-def:set	0..1	false	Enables the expression of complex wmi57_objects that are the result of logically combining and filtering the wmi57_items that are identified by one or more wmi57_objects.
namespace	oval-def:EntityObjectStringType	0..1	false	Specifies which WMI namespace to look under. Each WMI provider normally registers its own WMI namespace and then all its classes within that namespace[219].
wql	oval-def:EntityObjectStringType	0..1	false	A WQL query used to identify the wmi57_objects to represent as wmi57_items. Any valid WQL query is usable with one exception, all fields must be named in the SELECT portion of the query[220].
filter	oval-def:filter [2]	0..*	false	Allows for the explicit

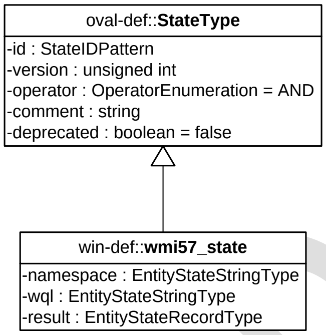
[219] For more information see http://msdn.microsoft.com/en-us/library/windows/desktop/aa394582%28v=vs.85%29.aspx

[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 platforms[221].


oval-def::**StateType**
-id : StateIDPattern
-version : unsigned int
-operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::**wmi57_state**
-namespace : EntityStateStringType
-wql : EntityStateStringType
-result : EntityStateRecordType

Property	Type	Multiplicity	Nillable	Description
namespace	oval-def: EntityStateStringType	0..1	false	Specifies which WMI namespace to look under. Each WMI provider normally registers its own WMI namespace and then all its classes within that namespace[222].

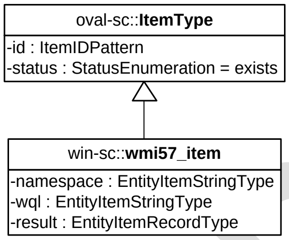
[221] For more information see http://msdn.microsoft.com/en-us/library/windows/desktop/aa394582%28v=vs.85%29.aspx

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

wql	oval-def: EntityStateStringType	0..1	false	A WQL query used to identify the `wmi57_objects` to represent as `wmi57_items`. Any valid WQL query is usable with one exception, all fields must be named in the SELECT portion of the query[223].
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.


oval-sc::ItemType
-id : ItemIDPattern
-status : StatusEnumeration = exists
win-sc::wmi57_item
-namespace : EntityItemStringType
-wql : EntityItemStringType
-result : EntityItemRecordType

Property	Type	Multiplicity	Nillable	Description
namespace	oval-sc:EntityItemStringType	0..1	false	Specifies which WMI namespace to look under. Each WMI provider normally registers its own WMI namespace and then all its classes within that namespace[224].
wql	oval-sc:EntityItemStringType	0..1	false	A WQL query used to identify

[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

				the wmi57_ objects to represent as wmi57_items. Any valid WQL query is usable with one exception, all fields must be named in the SELECT portion of the query[225].
result	oval-sc: EntityItemRecordType	0..*	false	The result attribute specifies how to test items in the result set of the specified WQL statement.

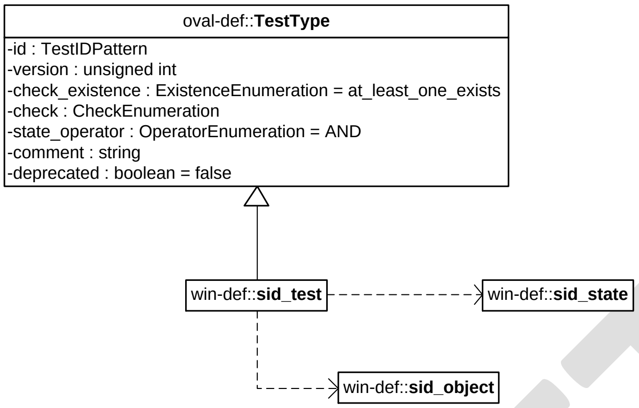
2.63. win-def:sid_test

The sid_test is used to make assertions about the properties associated with the specified trustee[226] name and its corresponding SID[227]. If a unique check is needed, use the sid_sid_test which matches based on the SID value, which is guaranteed to be unique. The sid_test MUST reference one sid_object and zero or more sid_states.

[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

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


oval-def::TestType
-id : TestIDPattern
-version : unsigned int
-check_existence : ExistenceEnumeration = at_least_one_exists
-check : CheckEnumeration
-state_operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::sid_test
win-def::sid_state
win-def::sid_object

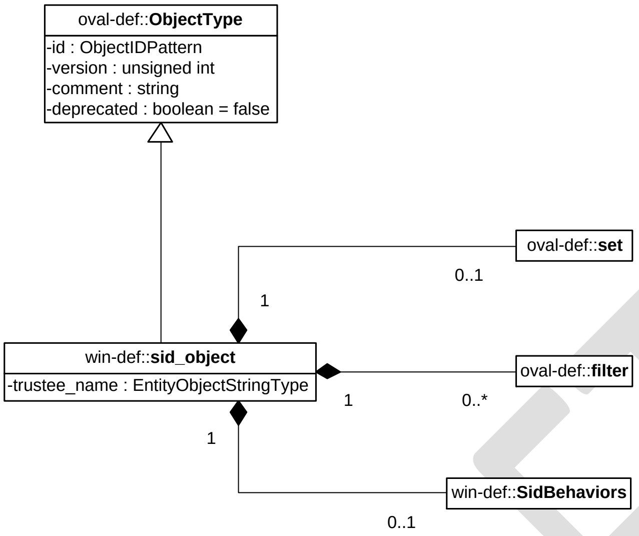
2.63.1. Known Supported Platforms

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



Property	Type	Multiplicity	Nillable	Description
set	oval-def:set	0..1	false	Enables the expression of complex sid_objects that are the result of logically combining and filtering the sid_items that are identified by one or more sid_objects.
behavior	win-def:SidBehaviors	0..1	false	Specifies the behaviors that direct how the sid_object collects sid_items from the system.
trustee_name	oval-def: EntityObjectStringType	1..1	false	The trustee_name attribute is the unique name (case-insensitive in Windows) that is associated to a particular SID. A SID can be associated with a user, group, or program (such as a Windows service). Because trustee names are case-insensitive, it is recommended that the case-insensitive operations are used for this property[229].

[229] For more information see 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 `sid_items` from the set of `sid_items` collected by a `sid_object`. 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.

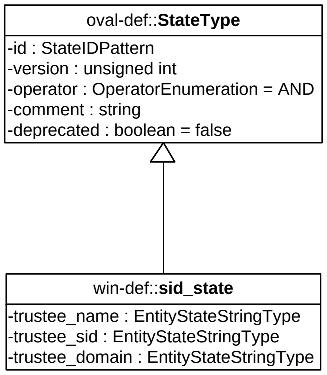
[230] For more information see http://msdn.microsoft.com/en-us/library/windows/desktop/aa379159%28v=VS.85%29.aspx

			Default Value: true
resolve_group	bool	*'true'* *'false'*	Defines whether or not the members of group SIDs should be resolved and collected. Note that all child groups should also be resolved and any valid domain accounts that are members should also be included. The intent of this behavior is to end up with a list of all individual users from that system that make up the group once everything has been resolved. *'true'*: The members of a group SID MUST be resolved and collected. 'false': The members of a group SID MUST NOT be resolved or collected. **Default Value: false**

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 platforms[231].

[231] For more information about trustees see http://msdn.microsoft.com/en-us/library/windows/desktop/aa379637(v=vs.85).aspx
For more information about SIDs see http://msdn.microsoft.com/en-us/library/windows/desktop/aa379571%28v=vs.85%29.aspx


oval-def::**StateType**
-id : StateIDPattern
-version : unsigned int
-operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::**sid_state**
-trustee_name : EntityStateStringType
-trustee_sid : EntityStateStringType
-trustee_domain : EntityStateStringType

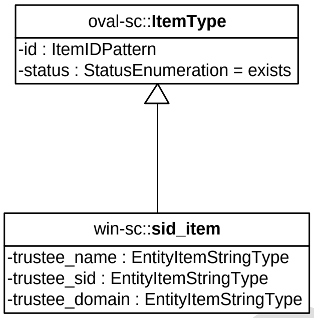
Property	Type	Multiplicity	Nillable	Description
trustee_name	oval-def: EntityStateStringType	0..1	false	The trustee_name property is the unique name (case-insensitive in Windows) that is associated to a particular SID. A SID can be associated with a user, group, or program (such as a Windows service). Because trustee names are case-insensitive, it is recommended that the case-insensitive operations are used for this attribute[232]. 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

[232] For more information see 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.


oval-sc::ItemType
-id : ItemIDPattern
-status : StatusEnumeration = exists
win-sc::sid_item
-trustee_name : EntityItemStringType
-trustee_sid : EntityItemStringType
-trustee_domain : EntityItemStringType

Property	Type	Multiplicity	Nillable	Description
trustee_name	oval-sc:EntityItemStringType	0..1	false	The trustee_name property is the unique name (case-insensitive in Windows) that is associated to a particular SID. A SID can be associated with a user, group, or program (such as a Windows service). Because trustee names are case-insensitive, it is recommended that the case-

[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

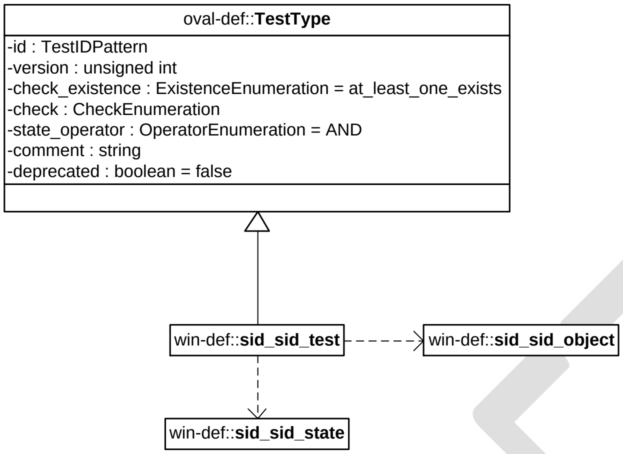
The `sid_sid_test` is used to check properties associated with the specified SID. Note that this test was added in version 5.4 as a temporary fix. There is a need within the community to identify objects like users and groups by both the name[236] and the SID[237]. The `sid_test` should be used instead when the object is identified by name. The `sid_sid_test` MUST reference one `sid_sid_object` and zero or more `sid_sid_states`.

[234] For more information see 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

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

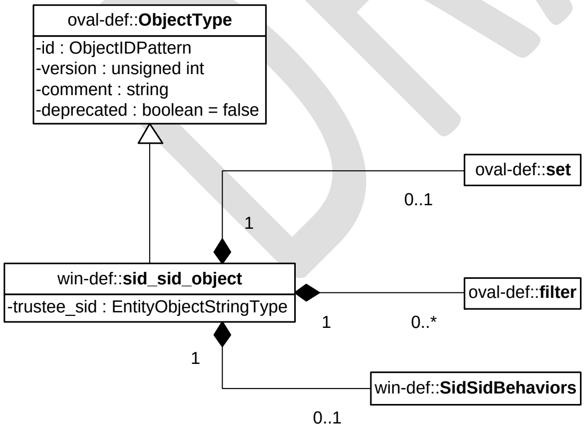

oval-def::TestType
-id : TestIDPattern
-version : unsigned int
-check_existence : ExistenceEnumeration = at_least_one_exists
-check : CheckEnumeration
-state_operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::sid_sid_test
win-def::sid_sid_object
win-def::sid_sid_state

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

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.

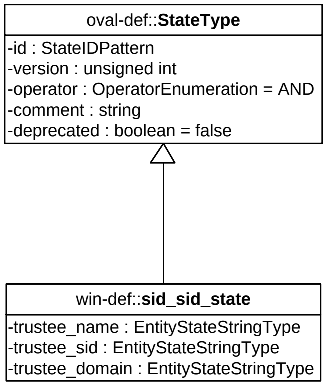
Attribute	Type	Possible Values	Description
include_group	boolean	*'true'* *'false'*	Defines whether or not the group SID should be collected when the trustee_sid property specifies a group SID. *'true'*: The group SID MUST be collected when the trustee_sid property specifies a group SID.

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

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

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.


oval-def::**StateType**
-id : StateIDPattern
-version : unsigned int
-operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::**sid_sid_state**
-trustee_name : EntityStateStringType
-trustee_sid : EntityStateStringType
-trustee_domain : EntityStateStringType

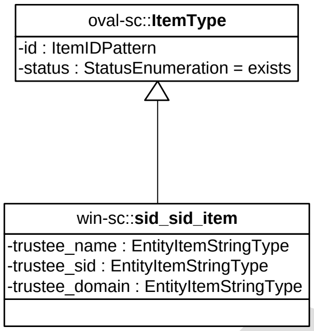
Property	Type	Multiplicity	Nillable	Description
trustee_name	oval-def: EntityStateStringType	0..1	false	The trustee_name property is the unique name (case-insensitive in Windows) that is associated to a particular SID. A SID can be associated with a user, group, or program (such as a Windows service). Because trustee names are case-insensitive, it is recommended that the case-insensitive operations are used for this property[239]. 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

[239] For more information see 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.


oval-sc::ItemType
-id : ItemIDPattern
-status : StatusEnumeration = exists
win-sc::sid_sid_item
-trustee_name : EntityItemStringType
-trustee_sid : EntityItemStringType
-trustee_domain : EntityItemStringType

Property	Type	Multiplicity	Nillable	Description
trustee_name	oval-sc: EntityItemStringType	0..1	false	The trustee_name property is the unique name (case-insensitive in Windows) that is associated to a particular SID. A SID can be associated with a user, group, or program (such as a Windows service). Because trustee names are case-insensitive, it is recommended that the case-insensitive operations are used for this property[241].

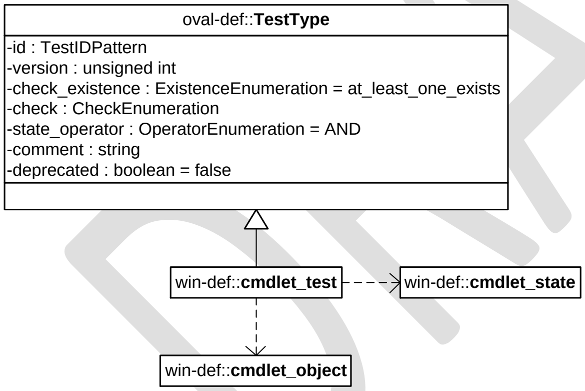
[240] For more information see http://msdn.microsoft.com/en-us/library/windows/desktop/aa379159%28v=VS.85%29.aspx

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

				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].


oval-def::TestType
-id : TestIDPattern
-version : unsigned int
-check_existence : ExistenceEnumeration = at_least_one_exists
-check : CheckEnumeration
-state_operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::cmdlet_test
win-def::cmdlet_state
win-def::cmdlet_object

2.73.1. Known Supported Platforms

- Windows XP
- Windows Vista
- Windows 7

Comment [DJH18]: We probably want to consider adding windows 2000, windows server 2003, windows server 2008, and windows server 2008 r2.

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

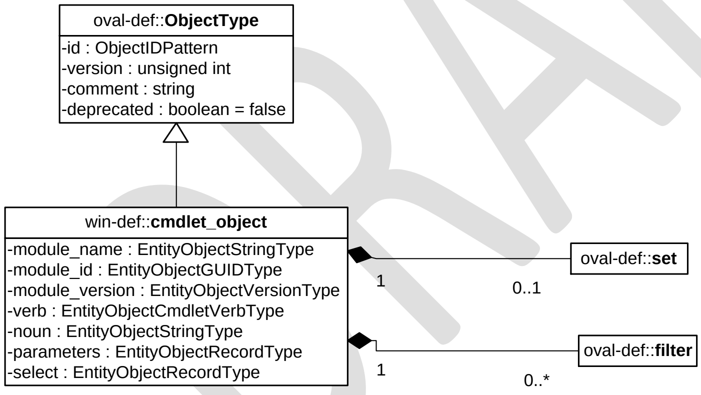
[243] For more information see http://msdn.microsoft.com/en-us/library/windows/desktop/ms714395(v=vs.85).aspx

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 Concepts[245]. Certain attributes (such as nouns, verbs, and parameter names) SHOULD align with the MSDN documentation[246].

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


oval-def::ObjectType
-id : ObjectIDPattern
-version : unsigned int
-comment : string
-deprecated : boolean = false
win-def::cmdlet_object
-module_name : EntityObjectStringType
-module_id : EntityObjectGUIDType
-module_version : EntityObjectVersionType
-verb : EntityObjectCmdletVerbType
-noun : EntityObjectStringType
-parameters : EntityObjectRecordType
-select : EntityObjectRecordType
oval-def::set
1
0..1
oval-def::filter
1
0..*

[244] For more information see 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
[246] For more information see 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	Nillable	Description
set	oval-def:set	0..1	false	Enables the expression of complex `cmdlet_objects` that are the result of logically combining and filtering the `cmdlet_items` that are identified by one or more `cmdlet_objects`.
module_name	oval-def:EntityObjectStringType	1..1	true	The name of the module that defines the cmdlet[248]. When set using the New-Module command in Powershell, the default name is __DynamicModule_PATHID where "PATHID" is a unique identifier that specifies the path to the dynamic module[249]. If **xsi:nil="true"**, it implies that it does not matter which module name the command comes from.
module_id	win-def:EntityObjectGUIDType	1..1	true	A global unique identifier (GUID) instituted so as to avoid module conflict. This is in the form A-B-C-D-E where A is an 8-digit hexadecimal number, B, C, and D are 4-digit hexadecimal numbers, and E is a 12-digit hexadecimal number[250]. If **xsi:nil="true"**, 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 *implies* an action even if that word is not a standard verb in the English language, such as *New*.
noun	oval-def: EntityObjectStringType	1..1	false	The noun name of the cmdlet[254]. 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

[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

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

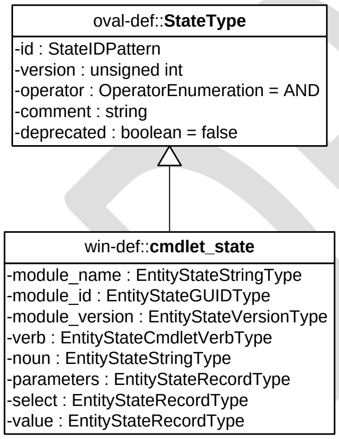
[257] For more information see http://msdn.microsoft.com/en-us/library/windows/desktop/dd878238(v=vs.85).aspx#RD03

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

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

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 documentation[260].


oval-def::StateType
-id : StateIDPattern
-version : unsigned int
-operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::cmdlet_state
-module_name : EntityStateStringType
-module_id : EntityStateGUIDType
-module_version : EntityStateVersionType
-verb : EntityStateCmdletVerbType
-noun : EntityStateStringType
-parameters : EntityStateRecordType
-select : EntityStateRecordType
-value : EntityStateRecordType

[259] For more information see 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

Property	Type	Multiplicity	Nillable	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 *implies* an action even if that word is not a standard verb in the English language, such as *New*.
noun	oval-def: EntityStateStringType	0..1	false	The noun name of the cmdlet[267]. 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

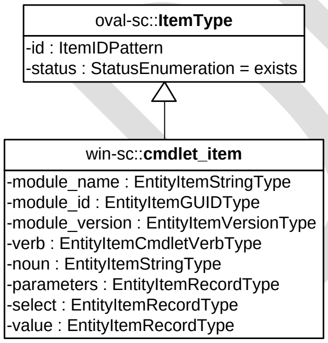
[261] For more information see http://www.microsoft.com/download/en/details.aspx?id=9706
[262] For more information see http://technet.microsoft.com/en-us/library/dd819471.aspx
[263] For more information see the examples in http://technet.microsoft.com/en-us/library/dd819471.aspx
[264] For more information 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
[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

				(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 returned[272]. Certain attributes (such as nouns, verbs, and parameter names) SHOULD align with the MSDN documentation[273].


oval-sc::ItemType
-id : ItemIDPattern
-status : StatusEnumeration = exists
win-sc::cmdlet_item
-module_name : EntityItemStringType
-module_id : EntityItemGUIDType
-module_version : EntityItemVersionType
-verb : EntityItemCmdletVerbType
-noun : EntityItemStringType
-parameters : EntityItemRecordType
-select : EntityItemRecordType
-value : EntityItemRecordType

[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

[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

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

Property	Type	Multiplicity	Nillable	Description
module_name	oval-sc:EntityItemStringType	0..1	true	The name of the module that defines the cmdlet[274]. When set using the New-Module command in Powershell, the default name is __DynamicModule_PATHID where "PATHID" is a unique identifier that specifies the path to the dynamic module[275]. If **xsi:nil="true"**, it implies that it does not matter which module name the command comes from.
module_id	win-sc:EntityItemGUIDType	0..1	true	A global unique identifier (GUID) instituted so as to avoid module conflict. This is in the form A-B-C-D-E where A is an 8-digit hexadecimal number, B, C, and D are 4-digit hexadecimal numbers, and E is a 12-digit hexadecimal number[276]. If **xsi:nil="true"**, it implies that it does not matter which module GUID the command comes from.
module_version	oval-sc:EntityItemVersionType	0..1	true	Module version in the format of MAJOR.MINOR[277]. If **xsi:nil="true"**, it implies that it does not matter which version of the module the command refers to.

[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 *implies* an action even if that word is not a standard verb in the English language, such as *New*.
noun	oval-sc:EntityItemStringType	0..1	false	The noun name of the cmdlet[280]. 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
[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
[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
[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]{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]{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]{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

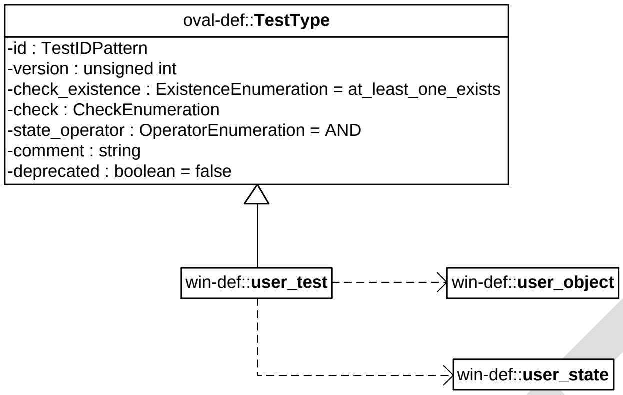
The EntityItemCmdletVerbType restricts a string value to a set of allow cmdlet verbs. The empty string is also allowed to support empty element associated with variable references. Note that when using pattern matches and variables care must be taken to ensure that the regular expression and variable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

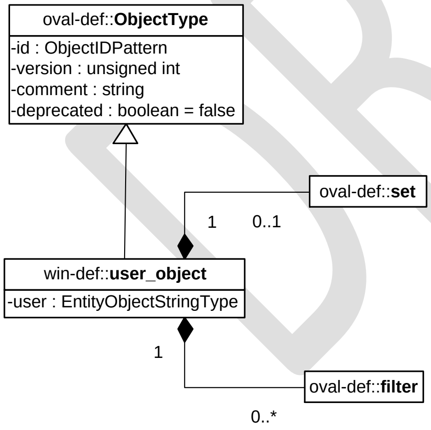

oval-def::TestType
-id : TestIDPattern
-version : unsigned int
-check_existence : ExistenceEnumeration = at_least_one_exists
-check : CheckEnumeration
-state_operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::user_test
win-def::user_object
win-def::user_state

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`.

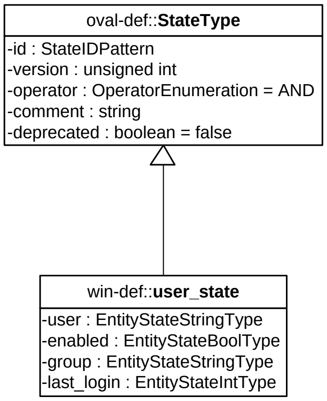


Property	Type	Multiplicity	Nillable	Description
set	oval-def:set	0..1	false	Enables the expression of complex user_objects that are the result of logically combining and filtering the user_items that are identified by one or more user_objects. Please see the OVAL Language Specification for additional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

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.

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


oval-def::**StateType**
-id : StateIDPattern
-version : unsigned int
-operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::**user_state**
-user : EntityStateStringType
-enabled : EntityStateBoolType
-group : EntityStateStringType
-last_login : EntityStateIntType

Property	Type	Multiplicity	Nillable	Description
user	oval-def: EntityStateStringType	0..1	false	The user property holds a case-insensitive string that represents the name of a particular user. In a domain environment, users SHOULD be identified in the form: "domain\user name". For local users use: "computer name\user name". For built-in accounts on the system, use the user name without a domain. User account names SHOULD align with the MSDN documentation[287]. In particular, user

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

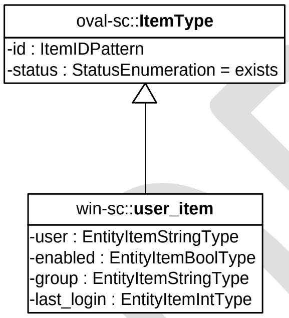
				account names in Windows are limited to 20 characters and SHOULD NOT contain the following illegal characters in the set {", /, \, [,], :, |, <, >, +, =, ;, ?, *}, any commas, or non-printable ASCII characters in the range 1-31.
enabled	oval-def:EntityStateBoolType	0..1	false	This property holds a boolean value that is *true* if the particular user account is enabled or *false* if it is not enabled.
group	oval-def: EntityStateStringType	0..1	false	A case insensitive string that represents the name of a particular group. In a domain environment, groups should be identified in the form: "domain\group name". For local groups use: "computer name\group name". For built-in accounts on the system, use the group name without a domain. Group names SHOULD align with the MSDN documentation[288]. In particular, group names in Windows are limited to 256 characters and SHOULD

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

				NOT contain the following illegal characters in the set {", /, \, [,], :, |, <, >, +, =, ;, ?, *}, any commas, or non-printable ASCII characters in the range 1-31.
last_login	oval-def:EntityStateIntType	0..1	true	The date and time when the last logon occurred. This value is stored as the number of seconds that have elapsed since 00:00:00, January 1, 1970, GMT.

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.


oval-sc::ItemType
-id : ItemIDPattern
-status : StatusEnumeration = exists
win-sc::user_item
-user : EntityItemStringType
-enabled : EntityItemBoolType
-group : EntityItemStringType
-last_login : EntityItemIntType

Property	Type	Multiplicity	Nillable	Description
user	oval-sc: EntityItemStringType	0..1	false	The user property holds a case-insensitive string that represents the name of a particular user. In a domain environment, users will be identified in the form: "domain\user name". For local users:

				"computer name\user name" is used. For built-in accounts on the system, the user name is used without a domain. User account names SHOULD align with the MSDN documentation[289]. In particular, user account names in Windows are limited to 20 characters and SHOULD NOT contain the following illegal characters in the set {", /, \, [,], :, |, <, >, +, =, ;, ?, *}, any commas, or non-printable ASCII characters in the range 1-31.
enabled	oval-sc: EntityItemBoolType	0..1	false	This element holds a boolean value that is *true* if the particular user account is enabled or *false* if it is not enabled.
group	oval-sc: EntityItemStringType	0..*	false	A string that represents the name of a particular group. The group element can be included multiple times in a system characteristic item in order to record that a user can be a member of a number of different groups. Group names SHOULD

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

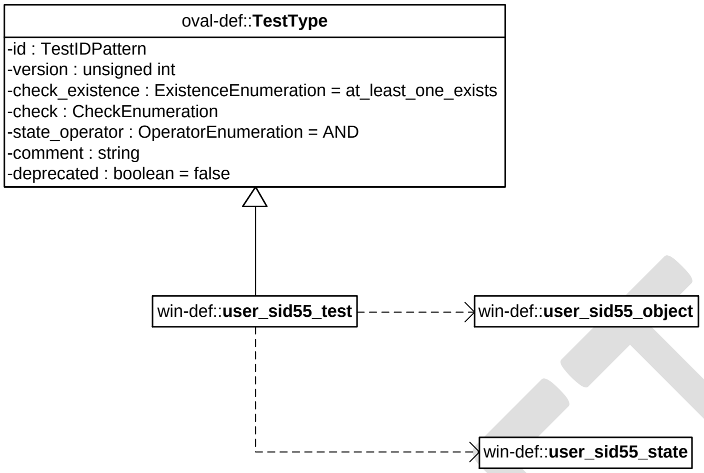
				align with the MSDN documentation[290]. In particular, group names in Windows are limited to 256 characters and SHOULD NOT contain the following illegal characters in the set {", /, \, [,], :, |, <, >, +, =, ;, ?, *}, any commas, or non-printable ASCII characters in the range 1-31.
last_login	oval-sc: EntityItemIntType	0..1	false	The date and time when the last logon occurred. This value is stored as the number of seconds that have elapsed since 00:00:00, January 1, 1970, GMT.

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].

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

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

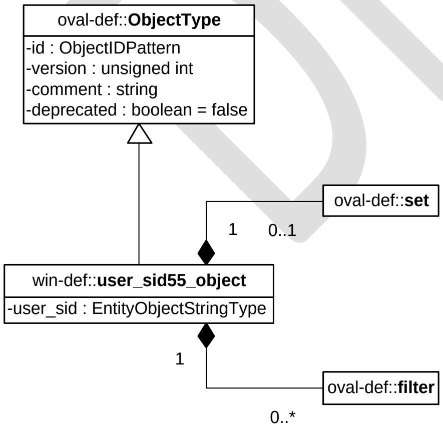

oval-def::TestType
-id : TestIDPattern
-version : unsigned int
-check_existence : ExistenceEnumeration = at_least_one_exists
-check : CheckEnumeration
-state_operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::user_sid55_test
win-def::user_sid55_object
win-def::user_sid55_state

2.87.1. Known Supported Platforms

- Windows XP
- Windows Vista
- Windows 7

2.88. win-def:user_sid55_object

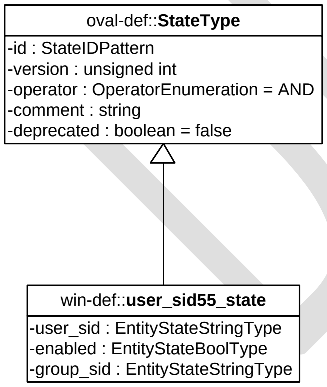
The `user_sid55_object` construct defines the set of users whose information should be collected and represented as `user_sid_items`.



Property	Type	Multiplicity	Nillable	Description
set	oval-def:set	0..1	false	Enables the expression of complex `user_sid55_objects` that are the result of logically combining and filtering the `user_sid_items` that are identified by one or more `user_sid55_objects`. Please see the OVAL Language Specification for additional information.
user_sid	oval-def:EntityObjectStringType	1..1	false	The user attribute holds a string that represents the SID of a particular user.
filter	oval-def:filter	0..*	false	Allows for the explicit inclusion or exclusion of `user_items` from the set of `user_items` collected by a `user_object`. Please see the OVAL Language Specification for additional information.

2.89. win-def:user_sid55_state

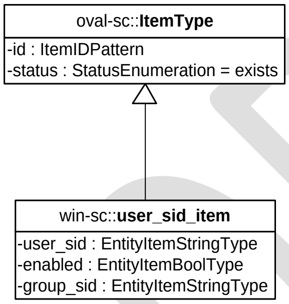
The `user_sid55_state` construct is used by a `user_sid55_test` to specify `user_sid_item` attribute criteria to check on Microsoft Windows platforms.


oval-def::StateType
-id : StateIDPattern
-version : unsigned int
-operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::user_sid55_state
-user_sid : EntityStateStringType
-enabled : EntityStateBoolType
-group_sid : EntityStateStringType

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

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.

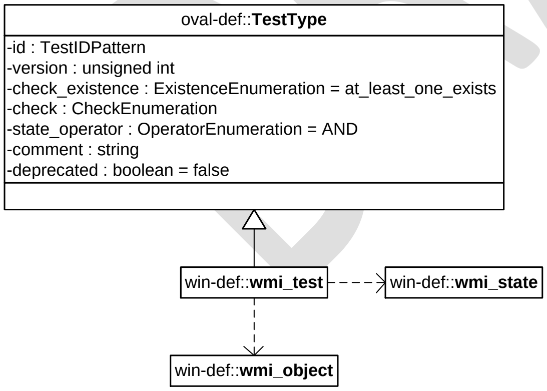

oval-sc::**ItemType**
-id : ItemIDPattern
-status : StatusEnumeration = exists
win-sc::**user_sid_item**
-user_sid : EntityItemStringType
-enabled : EntityItemBoolType
-group_sid : EntityItemStringType

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

group_sid	oval-sc: EntityItemStringType	0..*	false	A string that represents the SID of a group to which the user belongs.

2.91. win-def:wmi_test

The `wmi_test` is used to make assertions about information accessed by WMI[292]. The `wmi_test` MUST reference one `wmi_object` and zero or more `wmi_states`.


oval-def::TestType
-id : TestIDPattern
-version : unsigned int
-check_existence : ExistenceEnumeration = at_least_one_exists
-check : CheckEnumeration
-state_operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::wmi_test
win-def::wmi_state
win-def::wmi_object

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

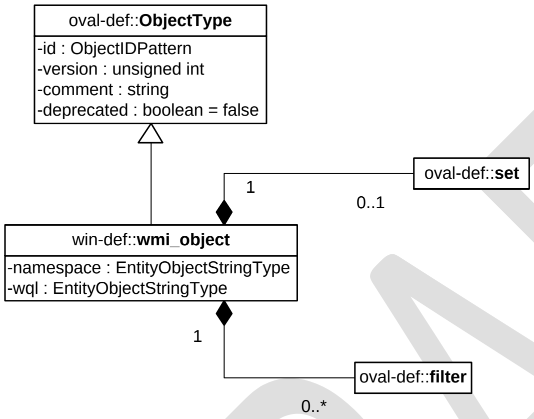
2.91.1. Known Supported Platforms

- Windows XP
- Windows Vista
- Windows 7

Comment [DJH19]: We probably want to consider adding windows 2000, windows server 2003, windows server 2008, and windows server 2008 r2.

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.



Property	Type	Multiplicity	Nillable	Description
set	oval-def:set	0..1	false	Enables the expression of complex `wmi57_objects` that are the result of logically combining and filtering the `wmi57_items` that are identified by one or more `wmi57_objects`.
namespace	oval-def:EntityObjectStringType	0..1	false	Specifies which WMI namespace to look under. Each WMI provider normally registers its own WMI namespace and then all its classes within that namespace[294].

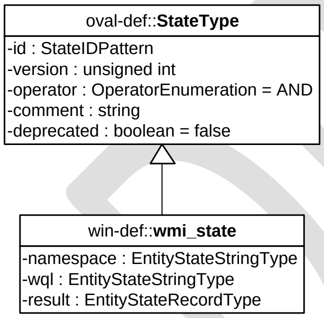
[293] For more information see http://msdn.microsoft.com/en-us/library/windows/desktop/aa394582%28v=vs.85%29.aspx

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

wql	oval-def:EntityObjectStringType	0..1	false	A WQL query used to identify the wmi_objects to represent as wmi_items. Any valid WQL query is usable with one exception, at most one field is allowed in the SELECT portion of the query[295].
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 platforms[296].


oval-def::StateType
-id : StateIDPattern
-version : unsigned int
-operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::wmi_state
-namespace : EntityStateStringType
-wql : EntityStateStringType
-result : EntityStateRecordType

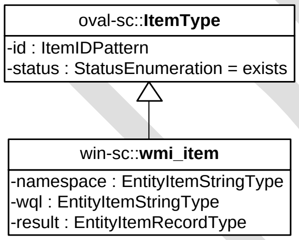
[295] For more information see http://msdn.microsoft.com/en-us/library/windows/desktop/aa394606%28v=vs.85%29.aspx

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

Property	Type	Multiplicity	Nillable	Description
namespace	oval-def: EntityStateStringType	0..1	false	Specifies which WMI namespace to look under. Each WMI provider normally registers its own WMI namespace and then all its classes within that namespace[297].
wql	oval-def: EntityStateStringType	0..1	false	A WQL query used to identify the `wmi_objects` to represent as `wmi_items`. Any valid WQL query is usable with one exception, at most one field is allowed in the SELECT portion of the query[298].
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.


oval-sc::ItemType
-id : ItemIDPattern
-status : StatusEnumeration = exists
win-sc::wmi_item
-namespace : EntityItemStringType
-wql : EntityItemStringType
-result : EntityItemRecordType

[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

Property	Type	Multiplicity	Nillable	Description
namespace	oval-sc: EntityItemStringType	0..1	false	Specifies which WMI namespace to look under. Each WMI provider normally registers its own WMI namespace and then all its classes within that namespace[299].
wql	oval-sc: EntityItemStringType	0..1	false	A WQL query used to identify the `wmi_objects` to represent as `wmi_items`. Any valid WQL query is usable with one exception, at most one field is allowed in the SELECT portion of the query[300].
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 groups[301]. A subgroup is an account identified by SID (not by name) that is of group type, which can be

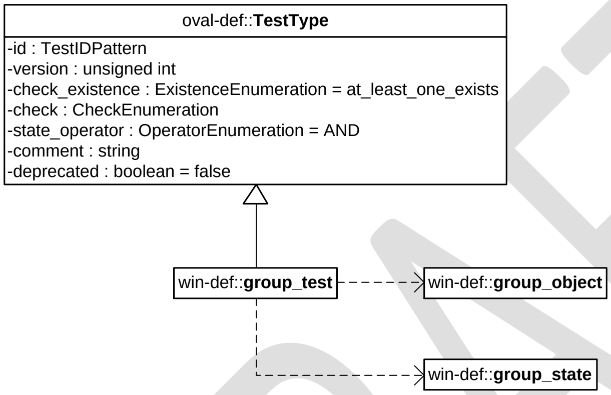
[299] For more information see http://msdn.microsoft.com/en-us/library/windows/desktop/aa394582%28v=vs.85%29.aspx

[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

seen when the SID_NAME_TYPE enumeration value of SidTypeGroup, or 2, is obtained when inputting a SID into the LookupAccountSid function[302].

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


oval-def::TestType
-id : TestIDPattern
-version : unsigned int
-check_existence : ExistenceEnumeration = at_least_one_exists
-check : CheckEnumeration
-state_operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::group_test
win-def::group_object
win-def::group_state

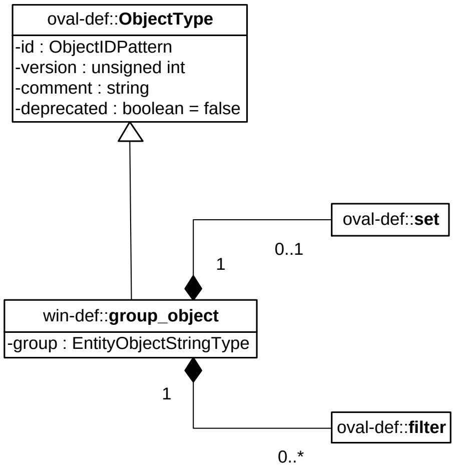
2.95.1. Known Supported Platforms

- 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.

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



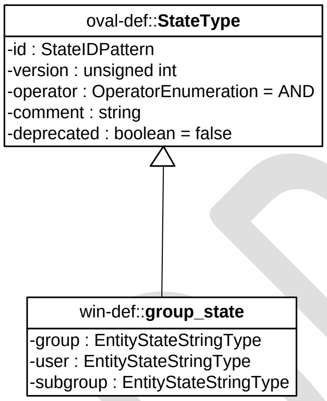
Property	Type	Multiplicity	Nillable	Description
set	oval-def:set	0..1	false	Enables the expression of complex `group_objects` that are the result of logically combining and filtering the `group_items` that are identified by one or more `group_objects`. Please see the OVAL Language Specification for additional information.
group	oval-def: EntityObjectStringType	1..1	false	A case insensitive string that represents the name of a particular group. In a domain environment, groups should be identified in the form: "domain\group name". For local groups use: "computer name\group name". For built-in accounts on the system, use the group name without a domain. Group names SHOULD align with the MSDN documentation[303]. In particular, group names in Windows are limited to 256 characters and SHOULD NOT contain the following illegal characters in the set {",

[303] For more information see the remarks section of 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 `group_items` from the set of `group_items` collected by a `group_object`. 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.


oval-def::StateType
-id : StateIDPattern
-version : unsigned int
-operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::group_state
-group : EntityStateStringType
-user : EntityStateStringType
-subgroup : EntityStateStringType

Property	Type	Multiplicity	Nillable	Description
group	oval-def: EntityStateStringType	0..1	false	A case insensitive string that represents the name of a particular group. In a domain environment, groups should be identified in the form: "domain\group name". For local groups use:

				"computer name\group name". For built-in accounts on the system, use the group name without a domain. Group names SHOULD align with the MSDN documentation[304]. In particular, group names in Windows are limited to 256 characters and SHOULD NOT contain the following illegal characters in the set {", /, \, [,], :, |, <, >, +, =, ;, ?, *}, any commas, or non-printable ASCII characters in the range 1-31.
user	oval-def: EntityStateStringType	0..1	false	A case-insensitive string that represents the name of a particular user. In a domain environment, users will be identified in the form: "domain\user name". For local users: "computer name\user name" is used. For built-in accounts on the system, the user name is used without a domain. User account names SHOULD align with the MSDN documentation[305]. In

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

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

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

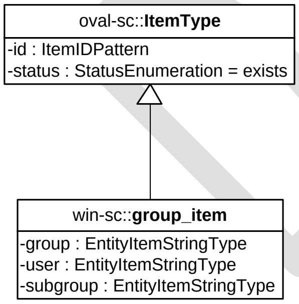
[306] For more information see the Remarks section of http://msdn.microsoft.com/en-us/library/windows/desktop/aa370653(v=vs.85).aspx

				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.

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'.


oval-sc::ItemType
-id : ItemIDPattern
-status : StatusEnumeration = exists
win-sc::group_item
-group : EntityItemStringType
-user : EntityItemStringType
-subgroup : EntityItemStringType

Property	Type	Multiplicity	Nillable	Description
group	oval-sc: EntityItemStringType	0..1	false	A case insensitive string that represents the name of a particular group.

				In a domain environment, groups should be identified in the form: "domain\group name". For local groups use: "computer name\group name". For built-in accounts on the system, use the group name without a domain. Group names SHOULD align with the MSDN documentation[307]. In particular, group names in Windows are limited to 256 characters and SHOULD NOT contain the following illegal characters in the set {", /, \, [,], :, |, <, >, +, =, ;, ?, *}, any commas, or non-printable ASCII characters in the range 1-31.
user	oval-sc: EntityItemStringType	0..*	false	A case-insensitive string that represents the name of a particular user. In a domain environment, users will be identified in the form: "domain\user name". For local users: "computer name\user name" is used. For built-in accounts on the system, the user name is used without a domain.

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

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

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

				MSDN documentation[309]. Thus, subgroup names are limited to 256 characters and SHOULD NOT contain the following illegal characters in the set {", /, \, [,], :, |, <, >, +, =, ;, ?, *}, any commas, or non-printable ASCII characters in the range 1-31.

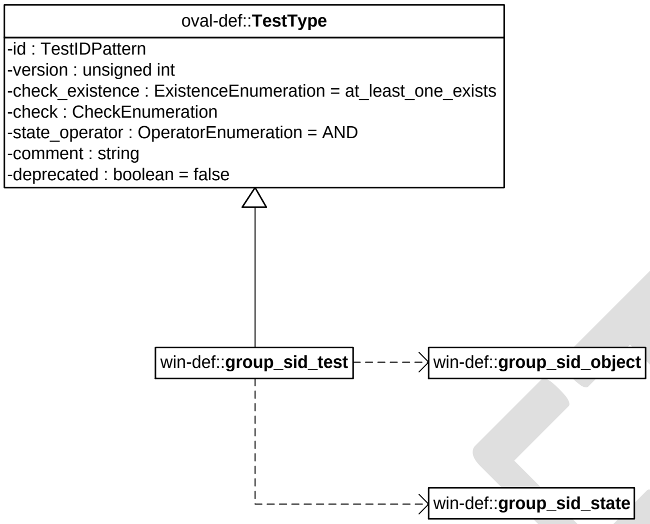
2.99. win-def:group_sid_test

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 function[310].

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

[309] For more information see the remarks section of 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
For more information about LookupAccountSid, see http://msdn.microsoft.com/en-us/library/windows/desktop/aa379166(v=vs.85).aspx

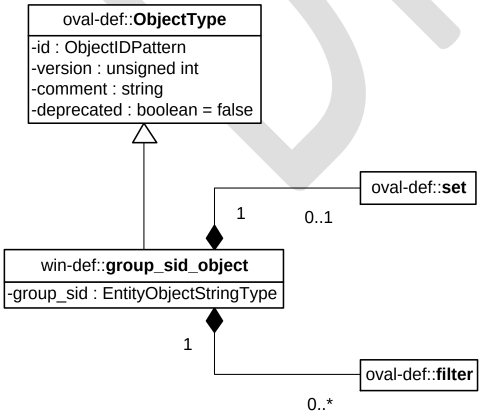

oval-def::TestType
-id : TestIDPattern
-version : unsigned int
-check_existence : ExistenceEnumeration = at_least_one_exists
-check : CheckEnumeration
-state_operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::group_sid_test
win-def::group_sid_object
win-def::group_sid_state

2.99.1. Known Supported Platforms

- Windows XP
- Windows Vista
- Windows 7

2.100. win-def:group_sid_object

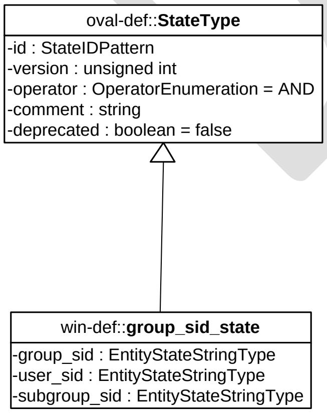
The `group_sid_object` is used by a `group_sid_test` to define the specific group(s) (identified by SID) to be evaluated and represented as `group_sid_items`.



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

2.101. win-def:group_sid_state

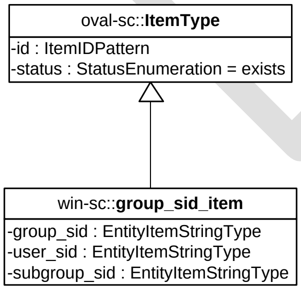
The group_sid_state construct is used by a group_sid_test to specify group_sid_item attribute criteria to check on Microsoft Windows platforms. This test enumerates the different users and subgroups directly associated with a Windows group.


oval-def::StateType
-id : StateIDPattern
-version : unsigned int
-operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::group_sid_state
-group_sid : EntityStateStringType
-user_sid : EntityStateStringType
-subgroup_sid : EntityStateStringType

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

2.102. win-sc:group_sid_item

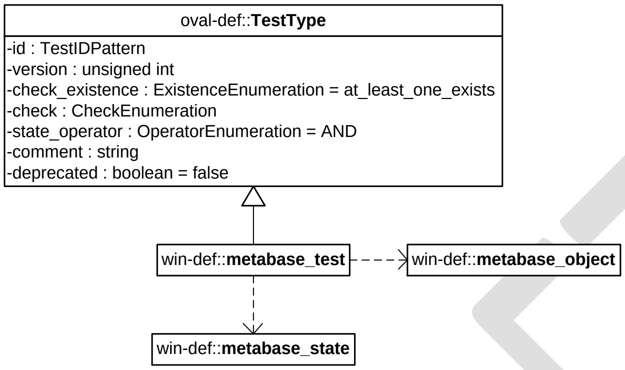
The Windows group_sid_item allows the different users and subgroups, that directly belong to specific groups (identified by SID), to be collected. The collected subgroups will not be resolved to find indirect user or subgroup members. If the subgroups need to be resolved, it should be done using the 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'.


oval-sc::ItemType
-id : ItemIDPattern
-status : StatusEnumeration = exists
win-sc::group_sid_item
-group_sid : EntityItemStringType
-user_sid : EntityItemStringType
-subgroup_sid : EntityItemStringType

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

2.103. win-def:metabase_test

The metabase_test is used to make assertions about information[311] found in the Windows metabase[312]. The metabase_test MUST reference one metabase_object and zero or more metabase_states.


oval-def::TestType
-id : TestIDPattern
-version : unsigned int
-check_existence : ExistenceEnumeration = at_least_one_exists
-check : CheckEnumeration
-state_operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::metabase_test
win-def::metabase_object
win-def::metabase_state

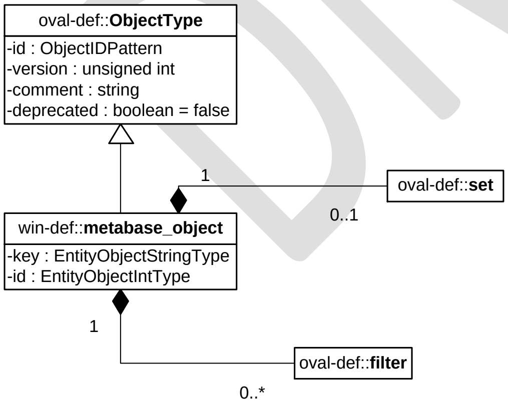
2.103.1. Known Supported Platforms

Comment [DJH20]: We probably want to consider adding windows 2000, windows server 2003, windows server 2008, and windows server 2008 r2.

- 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	Nillable	Description
set	oval-def:set	0..1	false	Enables the expression of complex `metabase_objects` that are the result of logically combining and filtering the `metabase_items` that are identified by one or more `metabase_objects`.
key	oval-def:EntityObjectStringType	0..1	false	This attribute specifies a metabase key[314].
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 id element SHOULD NOT be collected or used in analysis.
filter	oval-def:filter [2]	0..*	false	Allows for the explicit inclusion or exclusion of `metabase_items` from the set of `metabase_items` collected by a `metabase_object`. Please see the OVAL Language Specification [2] for additional information.

2.105. win-def:metabase_state

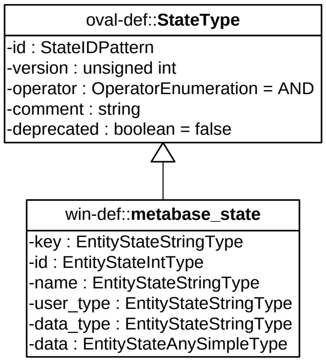
The `metabase_state` construct is used by a `metabase_test` to outline information to be checked through Microsoft's WMI interface. It specifies the applicable WMI information that can be associated with a given `metabase_object` under Microsoft Windows platforms. Some metabase properties can be found 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.

[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

[316] For more information see 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


oval-def::StateType
-id : StateIDPattern
-version : unsigned int
-operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::metabase_state
-key : EntityStateStringType
-id : EntityStateIntType
-name : EntityStateStringType
-user_type : EntityStateStringType
-data_type : EntityStateStringType
-data : EntityStateAnySimpleType

Property	Type	Multiplicity	Nillable	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: dwMDUserType. 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: dwMDDataType. The data_type element identifies 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

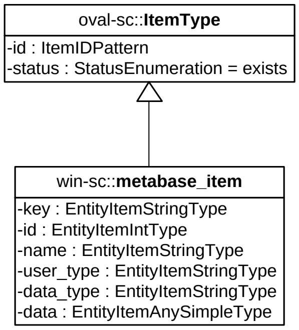
Comment [MS21]: Need a reference for what a metabase name might look like or where to find it.

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

				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 keys[324].


oval-sc::ItemType
-id : ItemIDPattern
-status : StatusEnumeration = exists
win-sc::metabase_item
-key : EntityItemStringType
-id : EntityItemIntType
-name : EntityItemStringType
-user_type : EntityItemStringType
-data_type : EntityItemStringType
-data : EntityItemAnySimpleType

Property	Type	Multiplicity	Nillable	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 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

Comment [MS22]: Need a reference for what a metabase name might look like or where to find it.

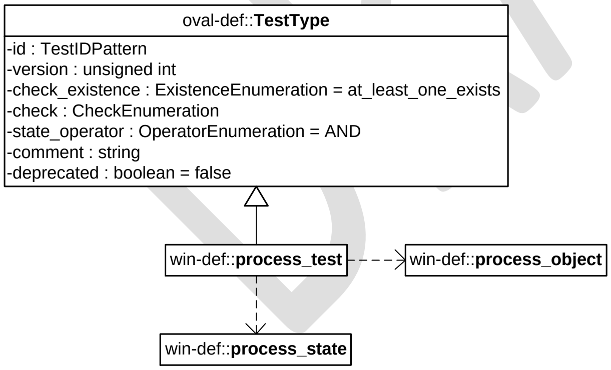
[323] For more information see http://msdn.microsoft.com/en-us/library/ms524951(v=vs.90).aspx
[324] For more information see http://msdn.microsoft.com/en-us/library/cc233554(v=PROT.10).aspx
[325] For more information see Metabase Concepts in http://technet.microsoft.com/en-us/query/ms524661
[326] For more information see Internal ID in http://msdn.microsoft.com/en-us/library/ms524578(v=vs.90).aspx#id
[327] For more information see http://msdn.microsoft.com/en-us/library/ms524635(v=VS.90).aspx

				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] .

2.107. win-def:process_test

The `process_test` is used to make assertions about information found in Windows processes[331].

The `process_test` MUST reference one `process_object` and zero or more `process_states`.


oval-def::**TestType**
-id : TestIDPattern
-version : unsigned int
-check_existence : ExistenceEnumeration = at_least_one_exists
-check : CheckEnumeration
-state_operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::**process_test**
win-def::**process_object**
win-def::**process_state**

[328] For more information see 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

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

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

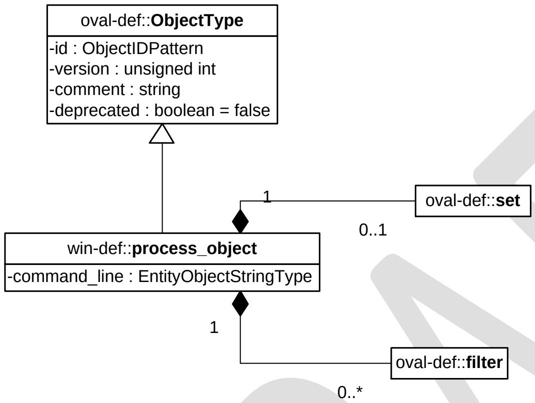
2.107.1. Known Supported Platforms

- Windows XP
- Windows Vista
- Windows 7

Comment [DJH23]: We probably want to consider adding windows 2000, windows server 2003, windows server 2008, and windows server 2008 r2.

2.108. win-def:process_object

The `process_object` construct defines the applicable process information that should be collected and represented as `process_items`.



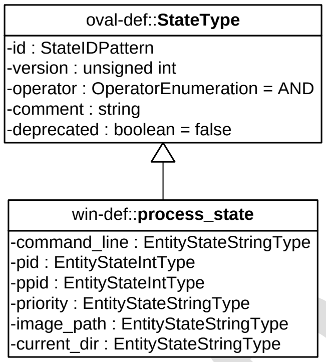
Property	Type	Multiplicity	Nillable	Description
set	oval-def:set	0..1	false	Enables the expression of complex `process_objects` that are the result of logically combining and filtering the `process_items` that are identified by one or more `process_objects`.
command_line	oval-def: EntityObjectStringType	0..1	false	The string used to start the process[332]. This includes any parameters that are part of the command line.
filter	oval-def:filter [2]	0..*	false	Allows for the explicit inclusion or exclusion of `process_items` from the set of `process_items` collected by a `process`

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

				_object. 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 processes[333]. By hitting CTRL-ALT-DELETE and clicking "Start Task Manager," a system administrator can view the contents of the properties specified here. If they are not shown, go to View->Select Columns… and select the fields corresponding to the "alternate names" mentioned here.


oval-def::StateType
-id : StateIDPattern
-version : unsigned int
-operator : OperatorEnumeration = AND
-comment : string
-deprecated : boolean = false
win-def::process_state
-command_line : EntityStateStringType
-pid : EntityStateIntType
-ppid : EntityStateIntType
-priority : EntityStateStringType
-image_path : EntityStateStringType
-current_dir : EntityStateStringType

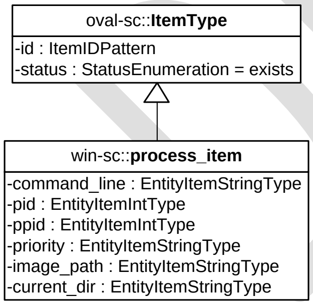
Property	Type	Multiplicity	Nillable	Description
command_line	oval-def: EntityStateStringType	0..1	false	Alternate name: Command Line. The string used to start the process[334]. This includes any parameters that are part of the command line.
pid	oval-def:EntityStateIntType	0..1	false	Alternate name: PID. 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.

[333] For more information see http://msdn.microsoft.com/en-us/library/windows/desktop/ms681917(v=VS.85).aspx
[334] For more information see http://msdn.microsoft.com/en-us/library/windows/desktop/aa394372(v=vs.85).aspx

image_path	oval-def: EntityStateStringType	0..1	false	Alternate name: Image Name. The name of the executable file in question. If it is 32-bit, the "Image Name" does not contain the "* 32" part of the name.
current_dir	oval-def: EntityStateStringType	0..1	false	Alternate name: Image Path Name, but without the file part. The current path to the executable, NOT including the exectable name itself. In other words, if y.exe was found in path x:\, then image_path would return y.exe and current_dir would return x:\. Image Path Name returns x:\y.exe in Task Manager.

2.110. win-sc:process_item

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


oval-sc::ItemType
-id : ItemIDPattern
-status : StatusEnumeration = exists
win-sc::process_item
-command_line : EntityItemStringType
-pid : EntityItemIntType
-ppid : EntityItemIntType
-priority : EntityItemStringType
-image_path : EntityItemStringType
-current_dir : EntityItemStringType

Property	Type	Multiplicity	Nillable	Description
command_line	oval-sc:	0..1	false	Alternate name: Command

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

	EntityItemStringType			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: EntityItemStringType	0..1	false	Alternate name: Image Name. The name of the executable file in question. If it is 32-bit, the "Image Name" does not contain the "* 32" part of the name.
current_dir	oval-sc: EntityItemStringType	0..1	false	Alternate name: Image Path Name, but without the file part. The current path to the executable, NOT including the exectable name itself. In other words, if y.exe was found in path x:\, then image_path would return y.exe and current_dir would return x:\. Image Path Name returns x:\y.exe in Task Manager.

Appendix A – Normative References

[1] RFC 2119 – Key words for use in RFCs to Indicate Requirement Levels
http://www.ietf.org/rfc/rfc2119.txt

[2] The OVAL Language Specification
http://oval.mitre.org/language/version5.10#specification

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

Appendix B - Change Log

Appendix C - Terms and Acronyms