- Open Vulnerability and Assessment Language - Element Dictionary

- Schema: Windows System Characteristics
- Version: 5.0 release candidate 3
- Release Date: 26 May 2006

The following is a description of the elements, types, and attributes that compose the Windows specific system characteristic items found in Open Vulnerability and Assessment Language (OVAL). Each item is an extension of the standard item element defined in the Core System Characteristic Schema. Through extension, each item inherits a set of elements and attributes that are shared amongst all OVAL Items. Each item is described in detail and should provide the information necessary to understand what each element and attribute represents. This document is intended for developers and assumes some familiarity with XML. A high level description of the interaction between the different tests and their relationship to the Core System Characteristic Schema is not outlined here.

The OVAL Schema is maintained by The Mitre Corporation and developed by the public OVAL Community. For more information, including how to get involved in the project and how to submit change requests, please visit the OVAL website at http://oval.mitre.org.

< accesstoken_item >

The access token item holds information about the individual privileges and rights associated with a specific access token. Each privilege and right in the data section accepts a boolean value signifying whether the privilege is granted or not. It extends the standard ItemType as defined in the oval-system-characteristics schema and one should refer to the ItemType description for more information.

Child Elements	Type	MinOccurs	MaxOccurs
security_principle	oval-sc:EntityItemStringType	0	1
seassignprimarytokenprivilege	oval-sc:EntityItemBoolType	0	1
seauditprivilege	oval-sc:EntityItemBoolType	0	1
sebackupprivilege	oval-sc:EntityItemBoolType	0	1
sechangenotifyprivilege	oval-sc:EntityItemBoolType	0	1
secreateglobalprivilege	oval-sc:EntityItemBoolType	0	1
secreatepagefileprivilege	oval-sc:EntityItemBoolType	0	1
secreatepermanentprivilege	oval-sc:EntityItemBoolType	0	1
secreatetokenprivilege	oval-sc:EntityItemBoolType	0	1
sedebugprivilege	oval-sc:EntityItemBoolType	0	1
seenabledelegationprivilege	oval-sc:EntityItemBoolType	0	1

seimpersonateprivilege	oval-sc:EntityItemBoolType	0	1
seincreasebasepriorityprivilege	oval-sc:EntityItemBoolType	0	1
seincreasequotaprivilege	oval-sc:EntityItemBoolType	0	1
seloaddriverprivilege	oval-sc:EntityItemBoolType	0	1
selockmemoryprivilege	oval-sc:EntityItemBoolType	0	1
semachineaccountprivilege	oval-sc:EntityItemBoolType	0	1
semanagevolumeprivilege	oval-sc:EntityItemBoolType	0	1
seprofilesingleprocessprivilege	oval-sc:EntityItemBoolType	0	1
seremoteshutdownprivilege	oval-sc:EntityItemBoolType	0	1
serestoreprivilege	oval-sc:EntityItemBoolType	0	1
sesecurityprivilege	oval-sc:EntityItemBoolType	0	1
seshutdownprivilege	oval-sc:EntityItemBoolType	0	1
sesyncagentprivilege	oval-sc:EntityItemBoolType	0	1
sesystemenvironmentprivilege	oval-sc:EntityItemBoolType	0	1
sesystemprofileprivilege	oval-sc:EntityItemBoolType	0	1
sesystemtimeprivilege	oval-sc:EntityItemBoolType	0	1
setakeownershipprivilege	oval-sc:EntityItemBoolType	0	1
setcbprivilege	oval-sc:EntityItemBoolType	0	1
seundockprivilege	oval-sc:EntityItemBoolType	0	1
seunsolicitedinputprivilege	oval-sc:EntityItemBoolType	0	1
sebatchlogonright	oval-sc:EntityItemBoolType	0	1
seinteractivelogonright	oval-sc:EntityItemBoolType	0	1
senetworklogonright	oval-sc:EntityItemBoolType	0	1
seremoteinteractivelogonright	oval-sc:EntityItemBoolType	0	1
seservicelogonright	oval-sc:EntityItemBoolType	0	1
sedenybatchLogonright	oval-sc:EntityItemBoolType	0	1
sedenyinteractivelogonright	oval-sc:EntityItemBoolType	0	1
sedenynetworklogonright	oval-sc:EntityItemBoolType	0	1
sedenyremoteInteractivelogonright	oval-sc:EntityItemBoolType	0	1
sedenyservicelogonright	oval-sc:EntityItemBoolType	0	1

< activedirectory_item >

The active directory item holds information about specific entries in the Windows Active Directory. It extends the standard ItemType as defined in the oval-system-characteristics schema and one should refer to the ItemType description for more information.

Child Elements	Type	MinOccurs	MaxOccurs
naming_context	win-sc:EntityItemNamingContextType	0	1
relative_dn	oval-sc:EntityItemStringType	0	1
attribute	oval-sc:EntityItemStringType	0	1
object_class	oval-sc:EntityItemStringType	0	1
adstype	win-sc:EntityItemAdstypeType	0	1
value	oval-sc:EntityItemAnyType	0	1

< auditeventpolicy_item >

The auditeventpolicy item enumerates the different types of events the system should audit. The defined values are found in window's POLICY_AUDIT_EVENT_TYPE enumeration and accessed through the LsaQueryInformationPolicy when the InformationClass parameters are set to PolicyAuditEventsInformation. It extends the standard ItemType as defined in the oval-system-characteristics schema and one should refer to the ItemType description for more information.

Child Elements	Type	MinOccurs	MaxOccurs
account_logon	win-sc:EntityItemAuditType	0	1
account_management	win-sc:EntityItemAuditType	0	1
detailed_tracking	win-sc:EntityItemAuditType	0	1
directory_service_access	win-sc:EntityItemAuditType	0	1
logon	win-sc:EntityItemAuditType	0	1
object_access	win-sc:EntityItemAuditType	0	1
policy_change	win-sc:EntityItemAuditType	0	1
privilege_use	win-sc:EntityItemAuditType	0	1
system	win-sc:EntityItemAuditType	0	1

< file_item >

This element stores file metadata. The time information can be retrieved by the _stst function.

Child Elements	Type	MinOccurs	MaxOccurs
path	oval-sc:EntityItemStringType	0	1
filename	oval-sc:EntityItemStringType	0	1
owner	oval-sc:EntityItemStringType	0	1
size	oval-sc:EntityItemIntType	0	1
a_time	oval-sc:EntityItemStringType	0	1
c_time	oval-sc:EntityItemStringType	0	1
m_time	oval-sc:EntityItemStringType	0	1
ms_checksum	oval-sc:EntityItemStringType	0	1
version	oval-sc:EntityItemStringType	0	1
type	win-sc:EntityItemFileTypeType	0	1
development_class	oval-sc:EntityItemStringType	0	1

< fileauditedpermissions_item >

This item stores the audited access rights of a file that a system access control list (SACL) structure grants to a specified trustee. The trustee's audited access rights are determined checking all access control entries (ACEs) in the SACL. For help with this test see the GetAuditedPermissionsFromAcl() api.

Child Elements	Type	MinOccurs	MaxOccurs
path	oval-sc:EntityItemStringType	0	1
filename	oval-sc:EntityItemStringType	0	1
trustee_name	oval-sc:EntityItemStringType	0	1
trustee_domain	oval-sc:EntityItemStringType	0	1
trustee_sid	oval-sc:EntityItemStringType	0	1
standard_delete	win-sc:EntityItemAuditType	0	1
standard_read_control	win-sc:EntityItemAuditType	0	1
standard_write_dac	win-sc:EntityItemAuditType	0	1
standard_write_owner	win-sc:EntityItemAuditType	0	1
standard_synchronize	win-sc:EntityItemAuditType	0	1
access_system_security	win-sc:EntityItemAuditType	0	1
generic_read	win-sc:EntityItemAuditType	0	1

generic_write	win-sc:EntityItemAuditType	0	1
generic_execute	win-sc:EntityItemAuditType	0	1
generic_all	win-sc:EntityItemAuditType	0	1
file_read_data	win-sc:EntityItemAuditType	0	1
file_write_data	win-sc:EntityItemAuditType	0	1
file_append_data	win-sc:EntityItemAuditType	0	1
file_read_ea	win-sc:EntityItemAuditType	0	1
file_write_ea	win-sc:EntityItemAuditType	0	1
file_execute	win-sc:EntityItemAuditType	0	1
file_delete_child	win-sc:EntityItemAuditType	0	1
file_read_attributes	win-sc:EntityItemAuditType	0	1
file_write_attributes	win-sc:EntityItemAuditType	0	1

< fileeffectiverights_item >

This item stores the effective rights of a file that a discretionary access control list (DACL) structure grants to a specified trustee. The trustee's effective rights are determined checking all access-allowed and access-denied access control entries (ACEs) in the DACL. For help with this test see the GetEffectiveRightsFromAcl() api.

Child Elements	Type	MinOccurs	MaxOccurs
path	oval-sc:EntityItemStringType	0	1
filename	oval-sc:EntityItemStringType	0	1
trustee_name	oval-sc:EntityItemStringType	0	1
trustee_domain	oval-sc:EntityItemStringType	0	1
trustee_sid	oval-sc:EntityItemStringType	0	1
standard_delete	oval-sc:EntityItemBoolType	0	1
standard_read_control	oval-sc:EntityItemBoolType	0	1
standard_write_dac	oval-sc:EntityItemBoolType	0	1
standard_write_owner	oval-sc:EntityItemBoolType	0	1
standard_synchronize	oval-sc:EntityItemBoolType	0	1
access_system_security	oval-sc:EntityItemBoolType	0	1
generic_read	oval-sc:EntityItemBoolType	0	1

generic_write	oval-sc:EntityItemBoolType	0	1
generic_execute	oval-sc:EntityItemBoolType	0	1
generic_all	oval-sc:EntityItemBoolType	0	1
file_read_data	oval-sc:EntityItemBoolType	0	1
file_write_data	oval-sc:EntityItemBoolType	0	1
file_append_data	oval-sc:EntityItemBoolType	0	1
file_read_ea	oval-sc:EntityItemBoolType	0	1
file_write_ea	oval-sc:EntityItemBoolType	0	1
file_execute	oval-sc:EntityItemBoolType	0	1
file_delete_child	oval-sc:EntityItemBoolType	0	1
file_read_attributes	oval-sc:EntityItemBoolType	0	1
file_write_attributes	oval-sc:EntityItemBoolType	0	1

< group_item >

The windows group item allows the different users that belong to specific groups be collected. Note that the user element can appear an unlimited number of times. If no user is found in the specified group, then a single user element should exist with a status of 'does not exist'. If there is an error determining the users of a group, then a single user element should exist with a status of 'error'.

Child Elements	Type	MinOccurs	MaxOccurs
group	oval-sc:EntityItemStringType	0	1
user	oval-sc:EntityItemStringType	0	unbounded

< interface_item >

Enumerate various attributes about the interfaces on a system.

Child Elements	Type	MinOccurs	MaxOccurs
name	oval-sc:EntityItemStringType	0	1
index	oval-sc:EntityItemIntType	0	1
type	win-sc:EntityItemInterfaceTypeType	0	1

hardware_addr	oval-sc:EntityItemStringType	0	1
inet_addr	oval-sc:EntityItemStringType	0	1
broadcast_addr	oval-sc:EntityItemStringType	0	1
netmask	oval-sc:EntityItemStringType	0	1
addr_type	win-sc:EntityItemAddrTypeType	0	unbounded

< lockoutpolicy_item >

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

Child Elements	Type	MinOccurs	MaxOccurs
force_logoff	oval-sc:EntityItemIntType	0	1
lockout_duration	oval-sc:EntityItemIntType	0	1
lockout_observation_window	oval-sc:EntityItemIntType	0	1
lockout_threshold	oval-sc:EntityItemIntType	0	1

< metabase_item >

This item gathers information from the specified metabase keys.

Child Elements	Type	MinOccurs	MaxOccurs
key	oval-sc:EntityItemStringType	0	1
id	oval-sc:EntityItemIntType	0	1
name	oval-sc:EntityItemStringType	0	1
user_type	oval-sc:EntityItemStringType	0	1
data_type	oval-sc:EntityItemStringType	0	1
data	oval-sc:EntityItemAnyType	0	unbounded

< passwordpolicy_item >

Specific policy items associated with passwords. Information is stored in the SAM or Active Directory but is encrypted or hidden so the registry_item and activedirectory_item are of no use. If this can be figured out, then the password_policy item is not needed.

Child Elements	Type	MinOccurs	MaxOccurs
max_passwd_age	oval-sc:EntityItemIntType	0	1
min_passwd_age	oval-sc:EntityItemIntType	0	1
min_passwd_len	oval-sc:EntityItemIntType	0	1
password_hist_len	oval-sc:EntityItemIntType	0	1
password_complexity	oval-sc:EntityItemBoolType	0	1
reversible_encryption	oval-sc:EntityItemBoolType	0	1

< port_item >

Information about open listening ports.

Child Elements	Type	MinOccurs	MaxOccurs
local_address	oval-sc:EntityItemStringType	0	1
local_port	oval-sc:EntityItemIntType	0	1
protocol	win-sc:EntityItemProtocolType	0	1
pid	oval-sc:EntityItemIntType	0	1

< process_item >

Information about running processes.

Child Elements	Type	MinOccurs	MaxOccurs
command_line	oval-sc:EntityItemStringType	0	1
pid	oval-sc:EntityItemIntType	0	1
ppid	oval-sc:EntityItemIntType	0	1
priority	oval-sc:EntityItemStringType	0	1

image_path	oval-sc:EntityItemStringType	0	1
current_dir	oval-sc:EntityItemStringType	0	1

< registry_item >

The windows registry item specifies a particular registry key (or keys) to collect.

Child Elements	Type	MinOccurs	MaxOccurs
hive	win-sc:EntityItemRegistryHiveType	0	1
key	oval-sc:EntityItemStringType	0	1
name	oval-sc:EntityItemStringType	0	1
type	win-sc:EntityItemRegistryTypeType	0	1
value	oval-sc:EntityItemAnyType	0	unbounded

< regkeyauditedpermissions_item >

This item stores the audited access rights of a registry key that a system access control list (SACL) structure grants to a specified trustee. The trustee's audited access rights are determined checking all access control entries (ACEs) in the SACL. For help with this test see the GetAuditedPermissionsFromAcl() api.

Child Elements	Type	MinOccurs	MaxOccurs
hive	win-sc:EntityItemRegistryHiveType	0	1
key	oval-sc:EntityItemStringType	0	1
trustee_name	oval-sc:EntityItemStringType	0	1
trustee_domain	oval-sc:EntityItemStringType	0	1
trustee_sid	oval-sc:EntityItemStringType	0	1
standard_delete	win-sc:EntityItemAuditType	0	1
standard_read_control	win-sc:EntityItemAuditType	0	1
standard_write_dac	win-sc:EntityItemAuditType	0	1
standard_write_owner	win-sc:EntityItemAuditType	0	1
standard_synchronize	win-sc:EntityItemAuditType	0	1

access_system_security	win-sc:EntityItemAuditType	0	1
generic_read	win-sc:EntityItemAuditType	0	1
generic_write	win-sc:EntityItemAuditType	0	1
generic_execute	win-sc:EntityItemAuditType	0	1
generic_all	win-sc:EntityItemAuditType	0	1
key_query_value	win-sc:EntityItemAuditType	0	1
key_set_value	win-sc:EntityItemAuditType	0	1
key_create_sub_key	win-sc:EntityItemAuditType	0	1
key_enumerate_sub_keys	win-sc:EntityItemAuditType	0	1
key_notify	win-sc:EntityItemAuditType	0	1
key_create_link	win-sc:EntityItemAuditType	0	1
key_wow64_64key	win-sc:EntityItemAuditType	0	1
key_wow64_32key	win-sc:EntityItemAuditType	0	1
key_wow64_res	win-sc:EntityItemAuditType	0	1

< regkeyeffectiverights_item >

This item stores the effective rights of a registry key that a discretionary access control list (DACL) structure grants to a specified trustee. The trustee's effective rights are determined checking all access-allowed and access-denied access control entries (ACEs) in the DACL. For help with this test see the GetEffectiveRightsFromAcl() api.

Child Elements	Type	MinOccurs	MaxOccurs
hive	win-sc:EntityItemRegistryHiveType	0	1
key	oval-sc:EntityItemStringType	0	1
trustee_name	oval-sc:EntityItemStringType	0	1
trustee_domain	oval-sc:EntityItemStringType	0	1
trustee_sid	oval-sc:EntityItemStringType	0	1
standard_delete	oval-sc:EntityItemBoolType	0	1
standard_read_control	oval-sc:EntityItemBoolType	0	1
standard_write_dac	oval-sc:EntityItemBoolType	0	1
standard_write_owner	oval-sc:EntityItemBoolType	0	1
standard_synchronize	oval-sc:EntityItemBoolType	0	1

access_system_security	oval-sc:EntityItemBoolType	0	1
generic_read	oval-sc:EntityItemBoolType	0	1
generic_write	oval-sc:EntityItemBoolType	0	1
generic_execute	oval-sc:EntityItemBoolType	0	1
generic_all	oval-sc:EntityItemBoolType	0	1
key_query_value	oval-sc:EntityItemBoolType	0	1
key_set_value	oval-sc:EntityItemBoolType	0	1
key_create_sub_key	oval-sc:EntityItemBoolType	0	1
key_enumerate_sub_keys	oval-sc:EntityItemBoolType	0	1
key_notify	oval-sc:EntityItemBoolType	0	1
key_create_link	oval-sc:EntityItemBoolType	0	1
key_wow64_64key	oval-sc:EntityItemBoolType	0	1
key_wow64_32key	oval-sc:EntityItemBoolType	0	1
key_wow64_res	oval-sc:EntityItemBoolType	0	1

< sid_item >

Child Elements	Type	MinOccurs	MaxOccurs
trustee_name	oval-sc:EntityItemStringType	0	1
trustee_sid	oval-sc:EntityItemBoolType	0	1
trustee_domain	oval-sc:EntityItemStringType	0	unbounded

< user_item >

The windows user item allows the different groups that a user belongs to be collected.

Child Elements	Type	MinOccurs	MaxOccurs
user	oval-sc:EntityItemStringType	0	1
enabled	oval-sc:EntityItemBoolType	0	1
group	oval-sc:EntityItemStringType	0	unbounded

< volume_item >

The volume item enumerates various attributes about a particular volume mounted to a machine. This includes the various system flags returned by GetVolumeInformation().

Child Elements	Type	MinOccurs	MaxOccurs
rootpath	oval-sc:EntityItemStringType	0	1
file_system	oval-sc:EntityItemStringType	0	1
name	oval-sc:EntityItemStringType	0	1
volume_max_component_length	oval-sc:EntityItemIntType	0	1
serial_number	oval-sc:EntityItemIntType	0	1
file_case_sensitive_search	oval-sc:EntityItemBoolType	0	1
file_case_preserved_names	oval-sc:EntityItemBoolType	0	1
file_unicode_on_disk	oval-sc:EntityItemBoolType	0	1
file_persistent_acls	oval-sc:EntityItemBoolType	0	1
file_file_compression	oval-sc:EntityItemBoolType	0	1
file_volume_quotas	oval-sc:EntityItemBoolType	0	1
file_supports_sparse_files	oval-sc:EntityItemBoolType	0	1
file_supports_reparse_points	oval-sc:EntityItemBoolType	0	1
file_supports_remote_storage	oval-sc:EntityItemBoolType	0	1
file_volume_is_compressed	oval-sc:EntityItemBoolType	0	1
file_supports_object_ids	oval-sc:EntityItemBoolType	0	1
file_supports_encryption	oval-sc:EntityItemBoolType	0	1
file_named_streams	oval-sc:EntityItemBoolType	0	1
file_read_only_volume	oval-sc:EntityItemBoolType	0	1

< wmi_item >

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

Child Elements	Type	MinOccurs	MaxOccurs

namespace	oval-sc:EntityItemStringType	0	1
wql	oval-sc:EntityItemStringType	0	1
result	oval-sc:EntityItemAnyType	0	unbounded

== EntityItemAddrTypeType ==

The EntityItemAddrTypeType restricts a string value to a specific set of values that describe the different address types of interfaces. The empty string is also allowed to support empty emlement associated with error conditions.

Value	Description
MIB_IPADDR_DELETED	
MIB_IPADDR_DISCONNECTED	
MIB_IPADDR_DYNAMIC	
MIB_IPADDR_PRIMARY	
MIB_IPADDR_TRANSIENT	

== EntityItemAdstypeType ==

The EntityItemAdstypeType restricts a string value to a specific set of values that describe the possible types associated with an Active Directory attribute. The empty string is also allowed to support empty emlement associated with error conditions.

Value	Description
ADSTYPE_INVALID	
ADSTYPE_DN_STRING	
ADSTYPE_CASE_EXACT_STRING	
ADSTYPE_CASE_IGNORE_STRIN	
ADSTYPE_PRINTABLE_STRING	
ADSTYPE_NUMERIC_STRING	
ADSTYPE_BOOLEAN	
ADSTYPE_INTEGER	
ADSTYPE_OCTET_STRING	

ADSTYPE_UTC_TIME
ADSTYPE_LARGE_INTEGER
ADSTYPE_PROV_SPECIFIC
ADSTYPE_OBJECT_CLASS
ADSTYPE_CASEIGNORE_LIST
ADSTYPE_OCTET_LIST
ADSTYPE_PATH
ADSTYPE_POSTALADDRESS
ADSTYPE_TIMESTAMP
ADSTYPE_BACKLINK
ADSTYPE_TYPEDNAME
ADSTYPE_HOLD
ADSTYPE_NETADDRESS
ADSTYPE_REPLICAPOINTER
ADSTYPE_FAXNUMBER
ADSTYPE_EMAIL
ADSTYPE_NT_SECURITY_DESCR
ADSTYPE_UNKNOWN
ADSTYPE_DN_WITH_BINARY
ADSTYPE_DN_WITH_STRING

== EntityItemAuditType ==

The EntityItemAuditType restricts a string value to a specific set of values: AUDIT_NONE, AUDIT_SUCCESS, AUDIT_FAILURE, and AUDIT_SUCCESS_FAILURE. These values describe which audit records should be generated. The empty string is also allowed to support empty emlement associated with error conditions.

Value	**Description**
AUDIT_FAILURE	
AUDIT_NONE	
AUDIT_SUCCESS	
AUDIT_SUCCESS_FAILURE	

== EntityItemFileTypeType ==

The EntityItemFileTypeType restricts a string value to a specific set of values that describe the different types of files. The empty string is also allowed to support empty emlement associated with error conditions.

Value	Description
FILE_ATTRIBUTE_DIRECTORY	
FILE_TYPE_CHAR	
FILE_TYPE_DISK	
FILE_TYPE_PIPE	
FILE_TYPE_REMOTE	
FILE_TYPE_UNKNOWN	

== EntityItemInterfaceTypeType ==

The EntityItemInterfaceTypeType restricts a string value to a specific set of values that describe the different types of interfaces. The empty string is also allowed to support empty emlement associated with error conditions.

Value	Description
MIB_IF_TYPE_ETHERNET	
MIB_IF_TYPE_FDDI	
MIB_IF_TYPE_LOOPBACK	
MIB_IF_TYPE_OTHER	
MIB_IF_TYPE_PPP	
MIB_IF_TYPE_SLIP	
MIB_IF_TYPE_TOKENRING	

== EntityItemNamingContextType ==

The EntityItemNamingContextType restricts a string value to a specific set of values: domain, configuration, and schema. These values describe the different naming context found withing Active Directory. The empty string is also allowed to support empty emlement associated with error conditions.

Value	Description
domain	
configuration	
schema	

== EntityItemProtocolType ==

The EntityItemProtocolType restricts a string value to a specific set of values that describe the different available protocols. The empty string is also allowed to support empty emlement associated with error conditions.

Value	Description
TCP	
UDP	

== EntityItemRegistryHiveType ==

The EntityItemRegistryHiveType restricts a string value to a specific set of values that describe the different registry hives. The empty string is also allowed to support empty emlement associated with error conditions.

Value	Description
HKEY_CLASSES_ROOT	
HKEY_CURRENT_CONFIG	
HKEY_CURRENT_USER	
HKEY_LOCAL_MACHINE	
HKEY_USERS	

== EntityItemRegistryTypeType ==

The EntityItemRegistryTypeType restricts a string value to a specific set of values that describe the different registry types. The empty string is also allowed to support empty emlement associated with error conditions.

Value	Description
reg_binary	

reg_dword
reg_expand_sz
reg_multi_sz
reg_qword
reg_sz