PC Policy Compliance

User Defined Control XML

Users of the Policy Compliance (PC) application have the ability to import & export user defined controls in XML format (see "User Permissions" below). User defined controls may be added to compliance policies and included in compliance reports just like system provided controls. This document describes the user defined control XML schema and required elements for various control types.

How To's

Export User Defined Controls Go to PC > Policies > Controls. Use the check boxes to select user defined controls you'd like to export. Then select Actions > Export. The selected controls will be saved in an XML file named "control_export_yyyymmdd.xml" using the schema ImportableControl.xsd. A maximum of 500 controls can be exported.

Import User Defined Controls Create user defined control(s) in an XML file using the schema ImportableControl.xsd. Go to PC > Policies > Controls. Then select New > Import from XML file and select the XML file with your user defined controls.

User Permissions. Users with the Manager and Auditor roles have permission to import and export user defined controls. Users with other roles (Unit Manager, Scanner and Reader) have permission to export user defined controls when the user has the "Manage compliance" permission; these users do not have permission to import controls.

XML Schema Definition. See ImportableControl.xsd to review the schema used to import and export user defined controls.

Important Notes. If a control exists in your account with the same description as control(s) being imported, the service assigns the DESCRIPTION parameter of the existing control to the DESCRIPTION parameter of all imported controls with the same scan parameters.

Sample - Windows Registry Key Existence Check

```
<CONTROL_LIST total="1">
    <CONTROL>
        <CHECK_TYPE>Registry Key Existence</CHECK_TYPE>
        <IS_CONTROL_DISABLE><![CDATA[0]]></IS_CONTROL_DISABLE>
        <CATEGORY>
            <ID>3</ID>
            <NAME><![CDATA[Access Control Requirements]]></NAME>
        </CATEGORY>
        <SUB_CATEGORY>
            <ID>1013</ID>
            <NAME><![CDATA[Authorizations (Multi-user ACL/role)]]></NAME>
        </SUB_CATEGORY>
        <STATEMENT><![CDATA[Permissions set for the
'%SystemRoot%\system32\regedt32.exe' file]]></STATEMENT>
        <CRITICALITY>
            <LABEL><![CDATA[SERIOUS]]></LABEL>
            <VALUE>3</VALUE>
        </CRITICALITY>
        <COMMENT><![CDATA[comment text]]></COMMENT>
            <IGNORE_ERROR>1</IGNORE_ERROR>
        <SCAN_PARAMETERS>
```

```
            <REG_HIVE><![CDATA[HKEY_CLASSES_ROOT (HKCR)]]></REG_HIVE>
            <REG_KEY><![CDATA[SOFTWARE\MICROSOFT]]></REG_KEY>
            <DATA_TYPE>Boolean</DATA_TYPE>
            <DESCRIPTION><![CDATA[The '%SystemRoot%\system32\regedt32.exe' executable
file launches a small program that runs the 'regedit.exe' program which is the
executable for the Windows Registry Editor that is used to import, export or delete
registry settings from a text (.REG) file.  The Windows registry is a directory which
stores settings and options for the operating system.  It also contains information and
settings for all the hardware, operating system software, most non-operating system
software, users and preferences of the system.  A user with permissions to 'regedit.exe'
has access to all the registry information and the ability to set/delete/modify keys
from a text (.REG) file.  Since this utility allows access to sensitive registry data,
permissions should be restricted to users requiring such privileged
access.]]></DESCRIPTION>
        </SCAN_PARAMETERS>
        <TECHNOLOGY_LIST total="1">
            <TECHNOLOGY>
                <ID>18</ID>
                <TECH_NAME><![CDATA[Windows Vista]]></TECH_NAME>
               <RATIONALE><![CDATA[The '%SystemRoot%\system32\regedt32.exe' executable
file launches a small program that runs the 'regedit.exe' program which is the
executable for the Windows Registry Editor that is used to import, export or delete
registry settings from a text (.REG) file.  The Windows registry is a directory which
stores settings and options for the operating system.  It also contains information and
settings for all the hardware, operating system software, most non-operating system
software, users and preferences of the system.  A user with permissions to 'regedit.exe'
has access to all the registry information and the ability to set/delete/modify keys
from a text (.REG) file.  Since this utility allows access to sensitive registry data,
permissions should be restricted to users requiring such privileged
access.]]></RATIONALE>
                <DATAPOINT>
                    <CARDINALITY>no cd</CARDINALITY>
                    <OPERATOR>no op</OPERATOR>
                    <DEFAULT_VALUES total="1">
                        <DEFAULT_VALUE>true</DEFAULT_VALUE>
                    </DEFAULT_VALUES>
                </DATAPOINT>
            </TECHNOLOGY>
        </TECHNOLOGY_LIST>
        <REFERENCE_LIST>
            <REFERENCE>
                <REF_DESCRIPTION><![CDATA[reference description]]></REF_DESCRIPTION>
                <URL><![CDATA[http://www.test.com/reference]]></URL>
            </REFERENCE>
        </REFERENCE_LIST>
    </CONTROL>
</CONTROL_LIST>
```

Sample - Unix Directory Search Check

```
<CONTROL_LIST total="1">
    <CONTROL>
        <ID>100027</ID>
        <UDC_ID>aac7a25a-67e9-7ca1-838c-03e98981451f</UDC_ID>
        <CHECK_TYPE>Unix Directory Search Check</CHECK_TYPE>
        <IS_CONTROL_DISABLE><![CDATA[0]]></IS_CONTROL_DISABLE>
        <CATEGORY>
            <ID>3</ID>
            <NAME><![CDATA[Access Control Requirements]]></NAME>
        </CATEGORY>
```

```
            <SUB_CATEGORY>
                <ID>1010</ID>
                <NAME><![CDATA[Account Creation/User Management]]></NAME>
            </SUB_CATEGORY>
            <STATEMENT><![CDATA[Directory Search-RHEL_Linux_UDC]]></STATEMENT>
            <CRITICALITY>
                <LABEL><![CDATA[SERIOUS]]></LABEL>
                <VALUE>3</VALUE>
            </CRITICALITY>
            <COMMENT><![CDATA[]]></COMMENT>
            <USE_AGENT_ONLY>1</USE_AGENT_ONLY>
            <IGNORE_ERROR>0</IGNORE_ERROR>
            <SCAN_PARAMETERS>
                <BASE_DIR><![CDATA[/root/UDC/Test/*]]></BASE_DIR>
                <SHOULD_DESCEND><![CDATA[false]]></SHOULD_DESCEND>
                <DEPTH_LIMIT><![CDATA[10]]></DEPTH_LIMIT>
                <FOLLOW_SYMLINK><![CDATA[true]]></FOLLOW_SYMLINK>
                <FILE_NAME_MATCH><![CDATA[*.conf]]></FILE_NAME_MATCH>
                <FILE_NAME_SKIP><![CDATA[]]></FILE_NAME_SKIP>
                <DIR_NAME_MATCH><![CDATA[*]]></DIR_NAME_MATCH>
                <DIR_NAME_SKIP><![CDATA[]]></DIR_NAME_SKIP>
                <PERMISSIONS>
                    <SPECIAL>
                        <USER>any</USER>
                        <GROUP>any</GROUP>
                        <DELETION>any</DELETION>
                    </SPECIAL>
                    <USER>
                        <READ>any</READ>
                        <WRITE>any</WRITE>
                        <EXECUTE>any</EXECUTE>
                    </USER>
                    <GROUP>
                        <READ>any</READ>
                        <WRITE>any</WRITE>
                        <EXECUTE>any</EXECUTE>
                    </GROUP>
                    <OTHER>
                        <READ>any</READ>
                        <WRITE>any</WRITE>
                        <EXECUTE>any</EXECUTE>
                    </OTHER>
                </PERMISSIONS>
                <PERM_COND><![CDATA[all]]></PERM_COND>
                <TYPE_MATCH><![CDATA[d,f,l,p,b,c,s]]></TYPE_MATCH>
                <USER_OWNER><![CDATA[Any User]]></USER_OWNER>
                <GROUP_OWNER><![CDATA[Any Group]]></GROUP_OWNER>
                <TIME_LIMIT><![CDATA[300]]></TIME_LIMIT>
                <MATCH_LIMIT><![CDATA[256]]></MATCH_LIMIT>
                <DATA_TYPE>String List</DATA_TYPE>
                <DESCRIPTION><![CDATA[Directory search check without giving any include or
        exclude directory path ]]></DESCRIPTION>
            </SCAN_PARAMETERS>
            <TECHNOLOGY_LIST total="5">
                <TECHNOLOGY>
                    <ID>35</ID>
                    <TECH_NAME><![CDATA[AIX 6.x]]></TECH_NAME>
                    <RATIONALE><![CDATA[Unix Directory Search ]]></RATIONALE>
                    <DATAPOINT>
                        <CARDINALITY>contains</CARDINALITY>
                        <OPERATOR>xre</OPERATOR>
```

```
                    <DEFAULT_VALUES total="1">
                        <DEFAULT_VALUE><![CDATA[*pass*]]></DEFAULT_VALUE>
                    </DEFAULT_VALUES>
                </DATAPOINT>
            </TECHNOLOGY>
            <TECHNOLOGY>
                <ID>45</ID>
                <TECH_NAME><![CDATA[Red Hat Enterprise Linux 6.x]]></TECH_NAME>
                <RATIONALE><![CDATA[Unix Directory Search ]]></RATIONALE>
                <DATAPOINT>
                    <CARDINALITY>does not contain</CARDINALITY>
                    <OPERATOR>xre</OPERATOR>
                    <DEFAULT_VALUES total="1">
                        <DEFAULT_VALUE><![CDATA[*pass*]]></DEFAULT_VALUE>
                    </DEFAULT_VALUES>
                </DATAPOINT>
            </TECHNOLOGY>
            <TECHNOLOGY>
                <ID>52</ID>
                <TECH_NAME><![CDATA[AIX 7.x]]></TECH_NAME>
                <RATIONALE><![CDATA[Unix Directory Search ]]></RATIONALE>
                <DATAPOINT>
                    <CARDINALITY>contains</CARDINALITY>
                    <OPERATOR>xre</OPERATOR>
                    <DEFAULT_VALUES total="1">
                        <DEFAULT_VALUE><![CDATA[*pass*]]></DEFAULT_VALUE>
                    </DEFAULT_VALUES>
                </DATAPOINT>
            </TECHNOLOGY>
            <TECHNOLOGY>
                <ID>80</ID>
                <TECH_NAME><![CDATA[CentOS 7.x]]></TECH_NAME>
                <RATIONALE><![CDATA[Unix Directory Search ]]></RATIONALE>
                <DATAPOINT>
                    <CARDINALITY>does not contain</CARDINALITY>
                    <OPERATOR>xre</OPERATOR>
                    <DEFAULT_VALUES total="1">
                        <DEFAULT_VALUE><![CDATA[*pass*]]></DEFAULT_VALUE>
                    </DEFAULT_VALUES>
                </DATAPOINT>
            </TECHNOLOGY>
            <TECHNOLOGY>
                <ID>81</ID>
                <TECH_NAME><![CDATA[Red Hat Enterprise Linux 7.x]]></TECH_NAME>
                <RATIONALE><![CDATA[Unix Directory Search ]]></RATIONALE>
                <DATAPOINT>
                    <CARDINALITY>does not contain</CARDINALITY>
                    <OPERATOR>xre</OPERATOR>
                    <DEFAULT_VALUES total="1">
                        <DEFAULT_VALUE><![CDATA[*pass*]]></DEFAULT_VALUE>
                    </DEFAULT_VALUES>
                </DATAPOINT>
            </TECHNOLOGY>
        </TECHNOLOGY_LIST>
        <REFERENCE_LIST/>
    </CONTROL>
</CONTROL_LIST>
```

Schema Elements

The table below describes the elements in the schema ImportableControl.xsd.

XML tag	Description
General	See Required Scan Parameters by Check Type
CHECK_TYPE	(Required) The check type: Registry Key Existence | Registry Value Existence | Registry Value Content Check | Registry Permission | Windows File Content Check | Windows File/Directory Existence | Windows File/Directory Permission | Unix File/Directory Permission | Unix File Content Check | Unix File/Directory Existence | Windows File Integrity Check | Unix File Integrity Check | WMI Query Check | Share Access Check | Unix Directory Search Check | Windows Directory Search Check | Windows Group Membership Check | Windows Directory Integrity Check | Unix Directory Integrity Check | MS SQL Database Check | Oracle Database Check | Sybase Database Check | PostgreSQL Database Check | SAP IQ Database Check | DB2 Database Check | Unix File Content Check V2
IS_CONTROL_DISABLE	(Optional) A value of 1 indicates that the control is disabled. A value of 0 indicates that the control is enabled.
ID	(Optional) An ID (integer) for a category, sub-category or technology, as defined by the service. The ID must be a number 1 - 999999999999999 (15 digits). Note: If a category ID is not provided, the service assigns the ID 1 (for OS Security Settings). If a sub-category is not provided, the service assigns the ID 1001 for System Settings (OSI layers 6-7).
NAME	(Optional) The name of a control category or sub-category; this value is assigned by the service automatically and cannot be customized. If you enter a custom name and then import the control XML, the custom name will not be saved. If specified, this value can have a maximum of 128 alphanumeric characters.
STATEMENT	(Required) A control statement that describes how the control should be implemented in the environment. This value can have a maximum of 1000 alphanumeric characters.
LABEL	(Optional) A label assigned to the control criticality (e.g. SERIOUS, CRITICAL, URGENT). When importing a control, we'll assign a label automatically based on the criticality value set in the <VALUE> tag. Define criticality settings for your subscription under PC > Policies > Setup > Control Criticality Levels.
VALUE	(Optional) A value (integer) assigned to the control criticality. The value can be a number 0-5. When importing a control, we'll use this value to set control criticality.
COMMENT	(Required) User-defined comments. This value can be a maximum of 1000 alphanumeric characters.
USE_AGENT_ONLY	(Optional for Directory Search checks and Directory Integrity checks, when Agent UDC Support is available) Specify 1 and we'll enable the "Use agent scan only" option for the control. When enabled, we'll evaluate the control using scan data collected from a cloud agent scan only. A value of 0 means this option is not enabled for the control.
Scan Parameters	See Required Scan Parameters by Check Type
DESCRIPTION	(Required) A description of the check's scan parameters. This value can be a maximum of 1000 alphanumeric characters.

XML tag	Description
FILE_PATH	(Optional) A scan parameter that identifies a pathname to a file or directory. This value can be a maximum of 1000 alphanumeric characters. This tag is required for any File/Directory check (not used for any Windows Registry check).
HASH_TYPE	(Optional) A scan parameter that identifies an algorithm to be used for computing a file hash: MD5 | SHA-1 | SHA-256. This tag is required for a Windows or Unix File Integrity Check.
Scan Parameters - Windows	See Required Scan Parameters by Check Type
REG_HIVE	(Optional) A scan parameter that identifies a Windows registry hive: HKEY_CLASSES_ROOT (HKCR) | HKEY_CURRENT_USER (HKCU) | HKEY_LOCAL_MACHINE (HKLM) | HKEY_USERS (HKU). This tag is required for Windows Registry check types.
REG_KEY	(Optional) A scan parameter that identifies a Windows registry key. This value can be a maximum of 1000 alphanumeric characters. This tag is required for any Windows Registry check type.
REG_VALUE_NAME	(Optional) A scan parameter that identifies a value for a Windows registry key. This value can be a maximum of 255 alphanumeric characters. This tag is required for Windows Registry Value Existence Check and Windows Registry Value Content Check.
WMI_NS	(Optional) A WMI namespace for a WMI query check. This value is case sensitive and it can have a maximum of 1000 characters. These characters may be included: a-z, A-Z, 0-9, \ (backslash), and _ (underscore). The namespace cannot include the hostname of a local or remote machine.
WMI_QUERY	(Optional) A WMI query for a WMI query check. This value can have a maximum of 4000 characters. WQL syntax if fully supported with these restrictions: 1) wildcard queries are not supported, and 2) REFLECTORS OF and ASSOCIATORS OF keywords are not supported.
SHARE_USER	(Optional) A user name who can access a share for a share access check. The user name may be in the format “user” or “domain\user”, and it can be a maximum of 256 alphanumeric characters. SHARE_USER or PATH_USER is required for a share access check.
PATH_USER	(Optional) A user name who can access a directory for a share access check. The user name may be in the format “user” or “domain\user”, and it can be a maximum of 256 alphanumeric characters. SHARE_USER or PATH_USER is required for a share access check.
Scan Parameters - Windows Directory Search Check	See Required Scan Parameters by Check Type
BASE_DIR	(Required) We’ll start the search from this directory (it must be a valid Windows directory). The directory name can be a maximum of 1000 characters.
DEPTH_LIMIT	(Optional) Select a depth level for searching each directory. Only directory contents (1) or multiple levels below the base directory (2-10). The default is 3.
FILE_NAME_MATCH	(Optional) Include files based on name. You’ll use a Windows wild-card expression. This can be a maximum of 255 characters.
FILE_NAME_SKIP	(Optional) Exclude files based on name. You’ll use a Windows wild-card expression. This can be a maximum of 255 characters.

XML tag	Description
DIR_NAME_MATCH	(Optional) Include directories based on name. You'll use a Windows wild-card expression. This can be a maximum of 1000 characters.
DIR_NAME_SKIP	(Optional) Exclude directories based on name. You'll use a Windows wild-card expression. This can be a maximum of 1000 characters.
TIME_LIMIT	(Optional) The search time limit, 30-900 seconds. The default is 300 seconds.
MATCH_LIMIT	(Optional) The maximum number of matches, 1-256 file objects. The default is 50.
WIN_FILE_SYS_OBJECT_TYPES	(Required) Specify at least one file system object type. Enter "Directory" to search directories, enter "File" to search files, or enter "Directory File" to search both.
MATCH_WELL_KNOWN_USERS_FOR_ANY_DOMAIN	(Optional) When set to "yes" (the default) we'll perform a look up of the users set in <WIN_PERMISSION_USERS> and match against well-known users, groups and aliases.
WIN_PERMISSION_USERS	(Required) A comma separated list of principals with permissions to the files/directories you want to match. You may include a mix of well-known users/groups and specific users. This can be 4000 characters max. Sample string: s-1-2-332-2222, AA,Windows Authorization Access Group,BA Use any of these formats to enter a specific user: user, domain\user, user@FQDN, SID (s-1-x-x-x-x-x-x...). You must enter abbreviated SDDL names for well-known users/groups, when available. For example, AU (authenticated users), BA (built-in administrators) and DD (domain controllers). We'll match these to well-known users when <MATCH_WELL_KNOWN_USERS_FOR_ANY_DOMAIN> is set to Yes. Click here to find abbreviated SDDL names for well-known users and groups.
WIN_PERMISSION_MATCH	(Required) Set to "any" (the default) to match principals with at least one of the permissions set in <WIN_BASIC_PERMISSIONS> or <WIN_ADVANCED_PERMISSIONS>. Set to "all" to only return files that match all of the permissions.
WIN_BASIC_PERMISSIONS	(Required) The set of basic file permissions you want to match. Specify each permission using <WIN_BASIC_PERMISSION_TYPE>.
WIN_BASIC_PERMISSION_TYPE	(Required) A basic permission: Full Control | Modify | List Folder | Content | Read & Execute | Write | Read.
WIN_ADVANCED_PERMISSIONS	(Required) The set of advanced file permissions you want to match. Specify each permission using <WIN_ADVANCED_PERMISSION_TYPE>.
WIN_ADVANCED_PERMISSION_TYPE	(Required) An advanced permission: Full Control | Traverse Folder/Execute Files | List Folder/Read Data | Read Attributes | Read Extended Attributes | Create Files/Write Data | Create Folders/Append Data | Write Attributes | Write Extended Attributes | Delete Sub-folders & Files | Delete | Read Permissions | Change Permissions | Take Ownership.
Scan Parameters - Windows Group Membership Check	See Required Scan Parameters by Check Type
GROUP_NAME	(Required) The local group name you want to get a list of members for.

XML tag	Description
GROUP_NAME_LIMIT	(Required) The maximum number of results (1 to 1000) you want returned for this group.
Scan Parameters - Windows Directory Integrity Check	See Required Scan Parameters by Check Type
BASE_DIR	(Required) We'll start the search from this directory (it must be a valid Windows directory). The directory name can be a maximum of 1000 characters.
INTEGRITY_CHECK_DEPTH_LIMIT	(Required) Select a depth level for searching each directory. Only directory contents (1) or multiple levels below the base directory (2-15). The default is 10.
FILE_NAME_MATCH	(Optional) Include files based on name. You'll use a Windows wild-card expression. This can be a maximum of 255 characters.
FILE_NAME_SKIP	(Optional) Exclude files based on name. You'll use a Windows wild-card expression. This can be a maximum of 255 characters.
DIR_NAME_MATCH	(Optional) Include directories based on name. You'll use a Windows wild-card expression. This can be a maximum of 1000 characters.
DIR_NAME_SKIP	(Optional) Exclude directories based on name. You'll use a Windows wild-card expression. This can be a maximum of 1000 characters.
INTEGRITY_CHECK_TIME_LIMIT	(Required) The search time limit, 60-1800 seconds. The default is 600 seconds.
INTEGRITY_CHECK_MATCH_LIMIT	(Required) The maximum number of matches, 1-2048. The default is 512.
INTEGRITY_CHECK_OBJECT_TYPES	(Optional) Include file system object types: f (regular file).
DIGEST_HASH	(Required) The algorithm you want to use to compute the digest: MD5, SHA-1 or SHA-256.
PERMISSION_MONITOR	(Optional) Enter "true" and we'll monitor permission changes and add to the digest used for control evaluation. Enter "false" (the default) and we will not monitor permission changes.
Scan Parameters - Unix	See Required Scan Parameters by Check Type
FILE_QUERY	(Optional) A scan parameter that identifies a query for a file content check. This value can be a maximum of 256 alphanumeric characters. This tag is required for a Unix File Content Check and Unix File Content Check V2.
Scan Parameters - Unix Directory Search Check	See Required Scan Parameters by Check Type
BASE_DIR	(Required) We'll start the search from this directory (it must be a valid Unix directory). The directory name can be a maximum of 1000 characters.
SHOULD_DESCEND	(Optional) Set to "true" to search into other file systems found. Selecting this option will likely increase scan time. Set to "false" (the default) and we won't search into other systems.
DEPTH_LIMIT	(Optional) Select a depth level for searching each directory. Only directory properties (0), directory contents (1) or multiple levels below the base directory (2-10). The default is 3.
FOLLOW_SYMLINK	(Optional) Set to "true" and we'll analyze target destination files and directories. Set to "false" (the default) to analyze the symbolic link itself (without following links).
FILE_NAME_MATCH	(Optional) Include files based on name. You'll use a globbing (wildcard) expression. This can be a maximum of 255 characters.

XML tag	Description
FILE_NAME_SKIP	(Optional) Exclude files based on name. You'll use a globbing (wildcard) expression. This can be a maximum of 255 characters.
DIR_NAME_MATCH	(Optional) Include directories based on name. You'll use a globbing (wildcard) expression. This can be a maximum of 1000 characters.
DIR_NAME_SKIP	(Optional) Exclude directories based on name. You'll use a globbing (wildcard) expression. This can be a maximum of 1000 characters.
PERMISSIONS	(Optional) Find files with certain permissions. Subelements are <SPECIAL>, <USER>, <GROUP>, <OTHER>.
PERM_COND	(Optional) Set to "all" (the default) to match all the permissions set in <PERMISSIONS>, set to "some" to match some of these permissions, or set to "exclude" to ignore files with specified permissions.
TYPE_MATCH	(Optional) Include file system object types by entering a comma separated string of codes: d (directory), f (regular file), l (symbolic link), p (named pipe, FIFO), b (block special - buffered), c (character special - unbuffered), s (socket), D (door, Solaris only). Sample string: d,f,l
USER_OWNER	(Optional) Find files owned or not owned by certain users. Specify a string with user names and/or UIDs, separated by commas.
GROUP_OWNER	(Optional) Find files owned or not owned by certain groups. Specify a string with group names and/or GUIDs, separated by commas.
EXCLUDE_USER_OWNER	(Optional, only supported by Cloud Agent) Set to "true" to exclude files owned by the specified users. Set to "false" (the default) and we won't exclude the files. When used, the scan data for the control evaluation is collected by the agent and then filtered by the agent.
EXCLUDE_GROUP_OWNER	(Optional, only supported by Cloud Agent) Set to "true" to exclude files owned by the specified groups. Set to "false" (the default) and we won't exclude the files. When used, the scan data for the control evaluation is collected by the agent and then filtered by the agent.
TIME_LIMIT	(Optional) The search time limit, 30-900 seconds. The default is 300 seconds.
MATCH_LIMIT	(Optional) The maximum number of matches, 1-256 file objects. The default is 50.
Scan Parameters - Unix Directory Integrity Check	See Required Scan Parameters by Check Type
BASE_DIR	(Required) We'll start the search from this directory (it must be a valid Unix directory). The directory name can be a maximum of 1000 characters.
SHOULD_DESCEND	(Optional) Set to "true" to search into other file systems found. Selecting this option will likely increase scan time. Set to "false" (the default) and we won't search into other systems.
INTEGRITY_CHECK_DEPTH_LIMIT	(Required) Select a depth level for searching each directory. Only directory properties (0), only directory contents (1) or multiple levels below the base directory (2-15). The default is 10.
FOLLOW_SYMLINK	(Optional) Set to "true" and we'll analyze target destination files and directories. Set to "false" (the default) to analyze the symbolic link itself (without following links).
FILE_NAME_MATCH	(Optional) Include files based on name. You'll use a globbing (wildcard) expression. This can be a maximum of 255 characters.

XML tag	Description
FILE_NAME_SKIP	(Optional) Exclude files based on name. You'll use a globbing (wildcard) expression. This can be a maximum of 255 characters.
DIR_NAME_MATCH	(Optional) Include directories based on name. You'll use a globbing (wildcard) expression. This can be a maximum of 1000 characters.
DIR_NAME_SKIP	(Optional) Exclude directories based on name. You'll use a globbing (wildcard) expression. This can be a maximum of 1000 characters.
TYPE_MATCH	(Optional) Include file system object types by entering a comma separated string of codes: d (directory), f (regular file), l (symbolic link), p (named pipe, FIFO), b (block special - buffered), c (character special - unbuffered), s (socket), D (door, Solaris only). Sample string: d,f,l
USER_OWNER	(Optional) Find files owned or not owned by certain users. Specify a string with user names and/or UIDs, separated by commas.
GROUP_OWNER	(Optional) Find files owned or not owned by certain groups. Specify a string with group names and/or GUIDs, separated by commas.
EXCLUDE_USER_OWNER	(Optional, only supported by Cloud Agent) Set to "true" to exclude files owned by the specified users. Set to "false" (the default) and we won't exclude the files. When used, the scan data for the control evaluation is collected by the agent and then filtered by the agent.
EXCLUDE_GROUP_OWNER	(Optional, only supported by Cloud Agent) Set to "true" to exclude files owned by the specified groups. Set to "false" (the default) and we won't exclude the files. When used, the scan data for the control evaluation is collected by the agent and then filtered by the agent.
INTEGRITY_CHECK_TIME_LIMIT	(Required) The search time limit, 60-1800 seconds. The default is 600 seconds.
INTEGRITY_CHECK_MATCH_LIMIT	(Required) The maximum number of matches, 1-2048. The default is 512.
DIGEST_HASH	(Required) The algorithm you want to use to compute the digest: MD5, SHA-1 or SHA-256.
Scan Parameters - Unix File Content Check V2	See Required Scan Parameters by Check Type
FILE_QUERY	(Required) A scan parameter that identifies a query for a file content check. This value can be a maximum of 256 alphanumeric characters.
BASE_DIR	(Required) We'll start the search from this directory (it must be a valid Unix directory). The directory name can be a maximum of 1000 characters.
DEPTH_LIMIT	(Optional) Select a depth level for searching each directory. Only directory properties (0), directory contents (1) or multiple levels below the base directory (2-10). The default is 3.
FOLLOW_SYMLINK	(Optional) Set to "true" and we'll analyze target destination files and directories. Set to "false" (the default) to analyze the symbolic link itself (without following links).
FILE_NAME_MATCH	(Optional) Include files based on name. You'll use a globbing (wildcard) expression. This can be a maximum of 255 characters.
FILE_NAME_SKIP	(Optional) Exclude files based on name. You'll use a globbing (wildcard) expression. This can be a maximum of 255 characters.
DIR_NAME_MATCH	(Optional) Include directories based on name. You'll use a globbing (wildcard) expression. This can be a maximum of 1000 characters.

XML tag	Description
DIR_NAME_SKIP	(Optional) Exclude directories based on name. You'll use a globbing (wildcard) expression. This can be a maximum of 1000 characters.
FILE_CONTENT_CHECK_V2_TIME_LIMIT	(Required) The search time limit, 60-1800 seconds. The default is 300 seconds.
FILE_CONTENT_CHECK_V2_MATCH_LIMIT	(Required) The maximum number of matches, 1-2048. The default is 50.
Control Technologies	See Control Values by Check Type
TECH_NAME	(Optional) The name of an applicable technology; this value is assigned by the service automatically and cannot be customized. If you enter a custom name and then import the control XML, the custom name will not be saved. If specified, this value can be a maximum of 64 alphanumeric characters.
RATIONALE	(Required) A rationale statement describing how the control should be implemented for each technology. This value can be a maximum of 4000 alphanumeric characters.
DATA_TYPE	(Required) A scan parameter that identifies a valid data type for the actual value provided by the service: Boolean | Integer | String | String List | Line List.
USE_SCAN_VALUE	(Required for File Integrity checks and Directory Integrity checks) Specify 1 and we'll set the expected value for the technology based on the actual value returned by the scan. A value of 0 means the default value is user specified.
DB_QUERY	(Required for MS SQL Database, Oracle Database, Sybase Database , and PostgreSQL/Pivotal Greenplum Database checks) Specify SQL statement to be executed on the database. This value can have a maximum of 32000 characters.
CARDINALITY	(Optional) A cardinality used to calculate the expected value for a technology. When DATA_TYPE is "String List": contains | does not contain | matches | is contained in | intersect. When DATA_TYPE is "Line List": match any | match all | match none | empty | not empty. When DATA_TYPE is "Boolean" or "Integer": no cd. below.
OPERATOR	(Optional) A name of an operator used to calculate the expected value for a technology: ge | gt | le | lt | ne | eq | in | range | re | xre | xeq | no op. See Operator Names below.
DEFAULT_VALUE	(Required) A default value for each technology. This is used to calculate the expected value for a technology, specified as a regular expression or a string depending on the check type. This value can be a maximum of 4000 alphanumeric characters. A regular expression must follow the PCRE Standard. See Regular Expressions below. See "Expected Value Calculations for Controls" in the online help to learn more.
IGNORE_ERROR	(Required) Set to 1 to ignore errors and mark the status as Passed; or set to 0 to process errors and mark the status as Error. By ignoring errors, the service marks control instances as Passed in cases where an error occurs during control evaluation.
IGNORE_ITEM_NOT_FOUND	(Required) Set to 1 to show a status of Passed or Failed in cases where a control returns error code 2 "item not found" (e.g. scan did not find file, registry, or related data, as appropriate for the control type); or set to 0 to not ignore status in these cases. When set to 1 we'll add a check box to the control in the policy where you'll set the status you prefer: Passed or Failed.

XML tag	Description
ERROR_SET_STATUS	(Optional) In cases of Database UDC, you can ignore errors and set status to Pass or Fail. By ignoring errors, the service marks control instances as Pass or Fail as per your selection, in cases where an error occurs during control evaluation.
REF_DESCRIPTION	(Optional) A user-defined description for a reference to an internal policy or document. This value can be a maximum of 2000 alphanumeric characters.
URL	(Optional) A URL for a reference to an internal policy or document. This value can be a maximum of 500 alphanumeric characters.

Required Scan Parameters by Check Type

The required scan parameters for each check type are shown below. These include registry, file or directory related parameter(s), the DATA_TYPE parameter and the DESCRIPTION parameter.

Check Type	Registry, File, Directory Parameters	Data Type
Registry Key Existence	REG_HIVE REG_KEY	Boolean
Registry Value Existence	REG_HIVE REG_KEY REG_VALUE_NAME	Boolean
Registry Value Content Check	REG_HIVE REG_KEY REG_VALUE_NAME	Boolean, Integer, String, or String List
Registry Permission	REG_HIVE REG_KEY	String List
Windows File Content Check	FILE_QUERY BASE_DIR REG_HIVE REG_KEY REG_VALUE_NAME FILE_PATH	String List
Windows File/Directory Existence	FILE_PATH	Boolean
Windows File/Directory Permission	FILE_PATH	String List
Windows File Integrity Check	FILE_PATH HASH_TYPE	String
Windows Group Membership Check	GROUP_NAME GROUP_NAME_LIMIT	String List
Windows WMI Query Check	WMI_NS WMI_QUERY	String List
Windows Share Access Check	SHARE_USER or PATH_USER	String List
Windows Directory Search Check*	BASE_DIR	String List
Windows Directory Integrity Check*	BASE_DIR DIGEST_HASH	String (when USE_SCAN_VALUE=1) String List (when USE_SCAN_VALUE=0)
Unix File/Directory Existence	FILE_PATH	Boolean
Unix File/Directory Permission	FILE_PATH	Boolean

Check Type	Registry, File, Directory Parameters	Data Type
Unix File Integrity Check	FILE_PATH HASH_TYPE	String
Unix File Content Check	FILE_PATH FILE_QUERY	Line List
Unix Directory Search Check*	BASE_DIR	String List
Unix Directory Integrity Check*	BASE_DIR DIGEST_HASH	String (when USE_SCAN_VALUE=1) String List (when USE_SCAN_VALUE=0)
Unix File Content Check V2	FILE_QUERY BASE_DIR FILE_CONTENT_CHECK_V2_TIME_LIMIT FILE_CONTENT_CHECK_V2_MATCH_LIMIT	String List

* Directory Search Checks and Directory Integrity Checks (Windows and Unix) have more scan parameters that are required. Please see the list of Scan Parameters for these check types.

Control Values by Check Type

The control values specify the method for calculating the expected value for a technology.

Check Type	Data Type	Supported Operators	Supported Cardinalities
Registry Key Existence	Boolean	no op	no cd
Registry Value Existence	Boolean	no op	no cd
Registry Value Content Check	Boolean	no op	no cd
	Integer	eq, lt, le, gt, ge, ne, in, range	no cd
	String	re	no cd
	String List	xre, xeq	contains, does not contain, matches, intersect, is contained in
Registry Permission	String List	xre, xeq	contains, does not contain, matches, intersect, is contained in
Windows File Content Check	String List	xre	contains, does not contain, matches, intersect, is contained in
Windows File/Directory Existence	Boolean	no op	no cd
Windows File/Directory Permission	String List	xre, xeq	contains, does not contain, matches, intersect, is contained in
Windows File Integrity Check	String	re	no cd

Check Type	Data Type	Supported Operators	Supported Cardinalities
Windows Group Membership Check	String List	xre, xeq	contains, does not contain, matches, intersect, is contained in
Windows WMI Query Check	String List	xre, xeq	contains, does not contain, matches, intersect, is contained in
Windows Share Access Check	String List	xre, xeq	contains, does not contain, matches, intersect, is contained in
Windows Directory Search Check	String List	xre, xeq	contains, does not contain, matches, intersect, is contained in
Windows Directory Integrity Check (when USE_SCAN_VALUE=1)	String	re	no cd
Windows Directory Integrity Check (when USE_SCAN_VALUE=0)	String List	xre, xeq	contains, match any, match all, match none, empty, not empty
Unix File/Directory Existence	Boolean	no op	no cd
Unix File/Directory Permission	String	re	no cd
Unix File Integrity Check	String	re	no cd
Unix File Content Check	Line List	re	match any, match all, match none, empty, not empty
Unix Directory Search Check	String List	xre, xeq	contains, does not contain, matches, intersect, is contained in
Unix Directory Integrity Check (when USE_SCAN_VALUE=1)	String	re	no cd
Unix Directory Integrity Check (when USE_SCAN_VALUE=0)	String List	xre, xeq	contains, match any, match all, match none, empty, not empty
Unix File Content Check V2	String List	xre, xeq	contains, does not contain, matches, intersect, is contained in

Operator Names

See below for a description of operator names.

Operator	Description	Operator	Description
ge	greater than or equal to	in	in
gt	greater than	range	in range
le	less than or equal to	re	regular expression
lt	less than	xre	regular expression list
eq	equal to	xeq	string list
ne	not equal to	no op	no operator

Regular Expressions

The PC application supports Perl Compatible Regular Expressions (PCRE) following the PCRE standard. For information on this standard, go to http://www.pcre.org/. For information on building proper regular expressions for controls using this standard, go to http://perldoc.perl.org/perlre.html.

ImportableControl.xsd

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">

    <xs:element name="CONTROL_LIST">
        <xs:complexType>
            <xs:sequence>
                <xs:element maxOccurs="unbounded" ref="CONTROL" />
            </xs:sequence>
            <xs:attribute name="total" use="required" type="xs:integer" />
        </xs:complexType>
    </xs:element>

    <xs:element name="ID" type="xs:integer" />

    <xs:element name="CONTROL">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="ID" minOccurs="0" maxOccurs="1" />
                <xs:element ref="UDC_ID" minOccurs="0" maxOccurs="1" />
                <xs:element ref="CHECK_TYPE" maxOccurs="1" />
                <xs:element ref="IS_CONTROL_DISABLE" minOccurs="0" maxOccurs="1" />
                <xs:element ref="CATEGORY" minOccurs="0" maxOccurs="1" />
                <xs:element ref="SUB_CATEGORY" minOccurs="0" maxOccurs="1" />
                <xs:element ref="STATEMENT" maxOccurs="1" />
                <xs:element ref="CRITICALITY" minOccurs="0" maxOccurs="1" />
                <xs:element ref="COMMENT" minOccurs="0" maxOccurs="1" />
                <xs:element ref="USE_AGENT_ONLY" minOccurs="0" maxOccurs="1" />
                <xs:element ref="AUTO_UPDATE" minOccurs="0" maxOccurs="1" />
                <xs:element ref="IGNORE_ERROR" minOccurs="0" maxOccurs="1" />
                <xs:element ref="ERROR_SET_STATUS" minOccurs="0" maxOccurs="1" />
                <xs:element ref="IGNORE_ITEM_NOT_FOUND" minOccurs="0" maxOccurs="1" />
                <xs:element ref="SCAN_PARAMETERS" minOccurs="0" maxOccurs="1" />
                <xs:element ref="TECHNOLOGY_LIST" maxOccurs="1" />
                <xs:element ref="REFERENCE_LIST" maxOccurs="1" />
            </xs:sequence>
        </xs:complexType>
    </xs:element>
```

```
<xs:element name="UDC_ID">
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:minLength value="0"/>
                <xs:maxLength value="36"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <xs:element name="CHECK_TYPE">
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:enumeration value="Registry Key Existence" />
                <xs:enumeration value="Registry Value Existence" />
                <xs:enumeration value="Registry Value Content Check" />
                <xs:enumeration value="Registry Permission" />
                <xs:enumeration value="Window File/Directory Existence" />
                <xs:enumeration value="Window File/Directory Permission" />
                <xs:enumeration value="Unix File/Directory Permission" />
                <xs:enumeration value="Unix File Content Check" />
                <xs:enumeration value="Unix File/Directory Existence" />
                <xs:enumeration value="Window File Integrity Check" />
                <xs:enumeration value="Unix File Integrity Check" />
                <xs:enumeration value="WMI Query Check" />
                <xs:enumeration value="Share Access Check" />
                <xs:enumeration value="Unix Directory Search Check" />
                <xs:enumeration value="Windows Directory Search Check" />
                <xs:enumeration value="Windows Group Membership Check" />
                <xs:enumeration value="Windows Directory Integrity Check" />
                <xs:enumeration value="Unix Directory Integrity Check" />
                <xs:enumeration value="MS SQL Database Check" />
                <xs:enumeration value="Oracle Database Check" />
                <xs:enumeration value="Sybase Database Check" />
                <xs:enumeration value="PostgreSQL Database Check" />
                <xs:enumeration value="SAP IQ Database Check" />
                <xs:enumeration value="Windows File Content Check" />
                <xs:enumeration value="DB2 Database Check" />
                <xs:enumeration value="Unix File Content Check V2" />
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <xs:element name="IS_CONTROL_DISABLE">
        <xs:simpleType>
            <xs:restriction base="xs:integer"/>
        </xs:simpleType>
    </xs:element>

    <xs:element name="CATEGORY">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="ID" minOccurs="0" maxOccurs="1"/>
                <xs:element name="NAME" minOccurs="0" maxOccurs="1" type="xs:string"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>

    <xs:element name="SUB_CATEGORY">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="ID"  minOccurs="0" maxOccurs="1"/>
```

```
            <xs:element ref="NAME" minOccurs="0" maxOccurs="1" />
        </xs:sequence>
    </xs:complexType>
</xs:element>

<xs:element name="CRITICALITY">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="LABEL" minOccurs="0" maxOccurs="1" />
            <xs:element ref="VALUE" minOccurs="0" maxOccurs="1" />
        </xs:sequence>
    </xs:complexType>
</xs:element>

<xs:element name="NAME">
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:minLength value="0"/>
            <xs:maxLength value="128"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="STATEMENT">
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:minLength value="1"/>
            <xs:maxLength value="1000"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="LABEL">
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:minLength value="1"/>
            <xs:maxLength value="16"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="VALUE">
    <xs:simpleType>
        <xs:restriction base="xs:integer">
            <xs:enumeration value="0" />
            <xs:enumeration value="1" />
            <xs:enumeration value="2" />
            <xs:enumeration value="3" />
            <xs:enumeration value="4" />
            <xs:enumeration value="5" />
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="COMMENT">
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:minLength value="0"/>
            <xs:maxLength value="1000"/>
        </xs:restriction>
    </xs:simpleType>
```

```
</xs:element>

<xs:element name="USE_AGENT_ONLY">
    <xs:simpleType>
        <xs:restriction base="xs:integer">
            <xs:enumeration value="0" />
            <xs:enumeration value="1" />
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="IGNORE_ERROR">
    <xs:simpleType>
        <xs:restriction base="xs:integer">
            <xs:enumeration value="0" />
            <xs:enumeration value="1" />
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="ERROR_SET_STATUS">
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:enumeration value="FAIL" />
            <xs:enumeration value="PASS" />
            <xs:enumeration value="" />
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="IGNORE_ITEM_NOT_FOUND">
    <xs:simpleType>
        <xs:restriction base="xs:integer">
            <xs:enumeration value="0" />
            <xs:enumeration value="1" />
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="AUTO_UPDATE">
    <xs:simpleType>
        <xs:restriction base="xs:integer">
            <xs:enumeration value="0" />
            <xs:enumeration value="1" />
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="SCAN_PARAMETERS">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="PATH_TYPE" minOccurs="0" maxOccurs="1" />
            <xs:element ref="REG_HIVE" minOccurs="0" maxOccurs="1" />
            <xs:element ref="REG_KEY" minOccurs="0" maxOccurs="1" />
            <xs:element ref="REG_VALUE_NAME" minOccurs="0" maxOccurs="1" />
            <xs:element ref="FILE_PATH" minOccurs="0" maxOccurs="1" />
            <xs:element ref="FILE_QUERY" minOccurs="0" maxOccurs="1" />
            <xs:element ref="HASH_TYPE" minOccurs="0" maxOccurs="1" />
            <xs:element ref="WMI_NS" minOccurs="0" maxOccurs="1" />
            <xs:element ref="WMI_QUERY" minOccurs="0" maxOccurs="1" />
            <xs:element ref="SHARE_USER" minOccurs="0" maxOccurs="1" />
```

```
                <xs:element ref="PATH_USER" minOccurs="0" maxOccurs="1" />
                <xs:element ref="BASE_DIR" minOccurs="0" maxOccurs="1" />
                <xs:element ref="SHOULD_DESCEND" minOccurs="0" maxOccurs="1" />
                <xs:element ref="DEPTH_LIMIT" minOccurs="0" maxOccurs="1" />
                <xs:element ref="INTEGRITY_CHECK_DEPTH_LIMIT" minOccurs="0"
maxOccurs="1" />
                <xs:element ref="FOLLOW_SYMLINK" minOccurs="0" maxOccurs="1" />
                <xs:element ref="FILE_NAME_MATCH" minOccurs="0" maxOccurs="1" />
                <xs:element ref="FILE_NAME_SKIP" minOccurs="0" maxOccurs="1" />
                <xs:element ref="DIR_NAME_MATCH" minOccurs="0" maxOccurs="1" />
                <xs:element ref="DIR_NAME_SKIP" minOccurs="0" maxOccurs="1" />
                <xs:element ref="PERMISSIONS" minOccurs="0" maxOccurs="1" />
                <xs:element ref="PERM_COND" minOccurs="0" maxOccurs="1" />
                <xs:element ref="TYPE_MATCH" minOccurs="0" maxOccurs="1" />
                <xs:element ref="USER_OWNER" minOccurs="0" maxOccurs="1" />
                <xs:element ref="GROUP_OWNER" minOccurs="0" maxOccurs="1" />
                <xs:element ref="TIME_LIMIT" minOccurs="0" maxOccurs="1" />
               <xs:element ref="INTEGRITY_CHECK_TIME_LIMIT" minOccurs="0" maxOccurs="1"
/>
                <xs:element ref="FILE_CONTENT_CHECK_V2_TIME_LIMIT" minOccurs="0"
maxOccurs="1" />
                <xs:element ref="MATCH_LIMIT" minOccurs="0" maxOccurs="1" />
                <xs:element ref="INTEGRITY_CHECK_MATCH_LIMIT" minOccurs="0"
maxOccurs="1" />
                <xs:element ref="FILE_CONTENT_CHECK_V2_MATCH_LIMIT" minOccurs="0"
maxOccurs="1" />
                <xs:element ref="WIN_FILE_SYS_OBJECT_TYPES" minOccurs="0" maxOccurs="1"
/>
                <xs:element ref="MATCH_WELL_KNOWN_USERS_FOR_ANY_DOMAIN" minOccurs="0"
maxOccurs="1" />
                <xs:element ref="WIN_PERMISSION_USERS" minOccurs="0" maxOccurs="1" />
                <xs:element ref="WIN_PERMISSION_MATCH" minOccurs="0" maxOccurs="1" />
                <xs:element ref="WIN_PERMISSIONS" minOccurs="0" maxOccurs="1" />
                <xs:element ref="GROUP_NAME" minOccurs="0" maxOccurs="1" />
                <xs:element ref="GROUP_NAME_LIMIT" minOccurs="0" maxOccurs="1" />
                <xs:element ref="INTEGRITY_CHECK_OBJECT_TYPES" minOccurs="0"
maxOccurs="1" />
                <xs:element ref="DISABLE_CASE_SENSITIVE_SEARCH" minOccurs="0"
maxOccurs="1" />
                <xs:element ref="EXCLUDE_USER_OWNER" minOccurs="0" maxOccurs="1" />
                <xs:element ref="EXCLUDE_GROUP_OWNER" minOccurs="0" maxOccurs="1" />
                <xs:element ref="DIGEST_HASH" minOccurs="0" maxOccurs="1" />
                <xs:element ref="PERMISSION_MONITOR" minOccurs="0" maxOccurs="1" />
                <xs:element ref="DATA_TYPE" maxOccurs="1" />
                <xs:element ref="EVALUATE_AS_STRING" minOccurs="0" maxOccurs="1" />
                <xs:element ref="DESCRIPTION" maxOccurs="1" />
            </xs:sequence>
        </xs:complexType>
    </xs:element>



    <xs:element name="REG_HIVE">
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:enumeration value="HKEY_CLASSES_ROOT (HKCR)" />
                <xs:enumeration value="HKEY_CURRENT_USER (HKCU)" />
                <xs:enumeration value="HKEY_LOCAL_MACHINE (HKLM)" />
                <xs:enumeration value="HKEY_USERS (HKU)" />
            </xs:restriction>
        </xs:simpleType>
```

```
</xs:element>

<xs:element name="REG_KEY">
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:minLength value="1"/>
            <xs:maxLength value="1000"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="REG_VALUE_NAME">
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:minLength value="1"/>
            <xs:maxLength value="255"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="FILE_PATH">
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:minLength value="0"/>
            <xs:maxLength value="1000"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="FILE_QUERY">
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:minLength value="1"/>
            <xs:maxLength value="256"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="HASH_TYPE">
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:enumeration value="MD5" />
            <xs:enumeration value="SHA-1" />
            <xs:enumeration value="SHA-256" />
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="WMI_NS">
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:minLength value="1"/>
            <xs:maxLength value="1000"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="WMI_QUERY">
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:minLength value="1"/>
```

```
            <xs:maxLength value="4000"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="SHARE_USER">
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:minLength value="1"/>
            <xs:maxLength value="256"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="PATH_USER">
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:minLength value="1"/>
            <xs:maxLength value="256"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="BASE_DIR">
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:minLength value="1"/>
            <xs:maxLength value="1000"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="SHOULD_DESCEND">
    <xs:simpleType>
        <xs:restriction base="xs:boolean">
            <xs:pattern value="true"/>
            <xs:pattern value="false"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="DEPTH_LIMIT">
    <xs:simpleType>
        <xs:restriction base="xs:integer">
            <xs:minInclusive value="0"/>
            <xs:maxInclusive value="10"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="INTEGRITY_CHECK_DEPTH_LIMIT">
    <xs:simpleType>
        <xs:restriction base="xs:integer">
            <xs:minInclusive value="0"/>
            <xs:maxInclusive value="15"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="FOLLOW_SYMLINK">
    <xs:simpleType>
```

```
            <xs:restriction base="xs:boolean">
                <xs:pattern value="true"/>
                <xs:pattern value="false"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <xs:element name="FILE_NAME_MATCH">
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:minLength value="0"/>
                <xs:maxLength value="4000"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <xs:element name="FILE_NAME_SKIP">
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:minLength value="0"/>
                <xs:maxLength value="40000"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <xs:element name="DIR_NAME_MATCH">
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:minLength value="0"/>
                <xs:maxLength value="4000"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <xs:element name="DIR_NAME_SKIP">
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:minLength value="0"/>
                <xs:maxLength value="4000"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <xs:element name="PERMISSIONS">
        <xs:complexType>
            <xs:sequence>
                <xs:element name="SPECIAL"  type="SPECIAL_OPTION" />
                <xs:element name="USER" type="PERM_OPTION" />
                <xs:element name="GROUP" type="PERM_OPTION" />
                <xs:element name="OTHER" type="PERM_OPTION" />
            </xs:sequence>
        </xs:complexType>
    </xs:element>

    <xs:complexType name="SPECIAL_OPTION">
        <xs:sequence>
            <xs:element name="USER"  type="PERM_TYPES" />
            <xs:element name="GROUP" type="PERM_TYPES" />
            <xs:element name="DELETION" type="PERM_TYPES" />
        </xs:sequence>
    </xs:complexType>
```

```
<xs:complexType name="PERM_OPTION">
    <xs:sequence>
        <xs:element name="READ"  type="PERM_TYPES" />
        <xs:element name="WRITE" type="PERM_TYPES" />
        <xs:element name="EXECUTE" type="PERM_TYPES" />
    </xs:sequence>
</xs:complexType>


<xs:simpleType name="PERM_TYPES">
    <xs:restriction base="xs:string">
        <xs:enumeration value="yes" />
        <xs:enumeration value="no" />
        <xs:enumeration value="any" />
    </xs:restriction>
</xs:simpleType>

<xs:element name="PERM_COND">
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:enumeration value="all" />
            <xs:enumeration value="some" />
            <xs:enumeration value="exclude" />
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="TYPE_MATCH">
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:minLength value="1"/>
            <xs:maxLength value="15"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="USER_OWNER">
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:minLength value="0"/>
            <xs:maxLength value="256"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="GROUP_OWNER">
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:minLength value="0"/>
            <xs:maxLength value="256"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="TIME_LIMIT">
    <xs:simpleType>
        <xs:restriction base="xs:integer">
            <xs:minInclusive value="30"/>
            <xs:maxInclusive value="900"/>
        </xs:restriction>
```

```
    </xs:simpleType>
</xs:element>

<xs:element name="INTEGRITY_CHECK_TIME_LIMIT">
    <xs:simpleType>
        <xs:restriction base="xs:integer">
            <xs:minInclusive value="60"/>
            <xs:maxInclusive value="1800"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="FILE_CONTENT_CHECK_V2_TIME_LIMIT">
    <xs:simpleType>
        <xs:restriction base="xs:integer">
            <xs:minInclusive value="60"/>
            <xs:maxInclusive value="1800"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>


<xs:element name="MATCH_LIMIT">
    <xs:simpleType>
        <xs:restriction base="xs:integer">
            <xs:minInclusive value="1"/>
            <xs:maxInclusive value="256"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="INTEGRITY_CHECK_MATCH_LIMIT">
    <xs:simpleType>
        <xs:restriction base="xs:integer">
            <xs:minInclusive value="1"/>
            <xs:maxInclusive value="2048"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="FILE_CONTENT_CHECK_V2_MATCH_LIMIT">
    <xs:simpleType>
        <xs:restriction base="xs:integer">
            <xs:minInclusive value="1"/>
            <xs:maxInclusive value="2048"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="WIN_PERMISSION_MATCH" >
    <xs:simpleType>
        <xs:restriction base="xs:token">
            <xs:enumeration value="Any" />
            <xs:enumeration value="All" />
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="MATCH_WELL_KNOWN_USERS_FOR_ANY_DOMAIN" type="yesOrNo" />
<xs:element name="WIN_PERMISSIONS">
    <xs:complexType>
```

```
            <xs:all>
                <xs:element name="WIN_BASIC_PERMISSIONS" type="winBasicPerms" />
                <xs:element name="WIN_ADVANCED_PERMISSIONS" type="winAdvPerms" />
            </xs:all>
        </xs:complexType>
    </xs:element>

    <xs:element name="WIN_FILE_SYS_OBJECT_TYPES">
        <xs:simpleType>
            <xs:list itemType="WIN_FILE_SYS_OBJECT_TYPE" />
        </xs:simpleType>
    </xs:element>

    <xs:simpleType name="WIN_FILE_SYS_OBJECT_TYPE">
        <xs:restriction base="xs:token">
            <xs:enumeration value="Directory" />
            <xs:enumeration value="File" />
            <xs:pattern value="Directory|File" />
        </xs:restriction>
    </xs:simpleType>

    <xs:element name="WIN_PERMISSION_USERS">
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:minLength value="0"/>
                <xs:maxLength value="4000"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <xs:element name="DISABLE_CASE_SENSITIVE_SEARCH">
        <xs:simpleType>
            <xs:restriction base="xs:boolean">
                <xs:pattern value="true"/>
                <xs:pattern value="false"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <xs:element name="EXCLUDE_USER_OWNER">
        <xs:simpleType>
            <xs:restriction base="xs:boolean">
                <xs:pattern value="true"/>
                <xs:pattern value="false"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <xs:element name="EXCLUDE_GROUP_OWNER">
        <xs:simpleType>
            <xs:restriction base="xs:boolean">
                <xs:pattern value="true"/>
                <xs:pattern value="false"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <xs:complexType name="winBasicPerms">
        <xs:choice>
            <xs:element ref="WIN_BASIC_PERMISSION_TYPE" minOccurs="1" maxOccurs="6" />
        </xs:choice>
```

```
        </xs:complexType>

        <xs:complexType name="winAdvPerms">
            <xs:sequence>
               <xs:element ref="WIN_ADVANCED_PERMISSION_TYPE" minOccurs="1" maxOccurs="14"
    />
            </xs:sequence>
        </xs:complexType>

        <xs:element name="WIN_BASIC_PERMISSION_TYPE">
            <xs:simpleType>
                <xs:restriction base="xs:token">
                    <xs:enumeration value="Full Control" />
                    <xs:enumeration value="Modify" />
                    <xs:enumeration value="List Folder Content" />
                    <xs:enumeration value="Read &amp; Execute" />
                    <xs:enumeration value="Write" />
                    <xs:enumeration value="Read" />
                </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <xs:element name="WIN_ADVANCED_PERMISSION_TYPE">
            <xs:simpleType>
                <xs:restriction base="xs:token">
                    <xs:enumeration value="Full Control" />
                    <xs:enumeration value="Traverse Folder / Execute Files" />
                    <xs:enumeration value="List Folder / Read Data" />
                    <xs:enumeration value="Read Attributes" />
                    <xs:enumeration value="Read Extended Attributes" />
                    <xs:enumeration value="Create Files / Write Data" />
                    <xs:enumeration value="Create Folders / Append Data" />
                    <xs:enumeration value="Write Attributes" />
                    <xs:enumeration value="Write Extended Attributes" />
                    <xs:enumeration value="Delete Sub-folders &amp; Files" />
                    <xs:enumeration value="Delete" />
                    <xs:enumeration value="Read Permissions" />
                    <xs:enumeration value="Change Permissions" />
                    <xs:enumeration value="Take Ownership" />
                </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <xs:element name="GROUP_NAME">
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:minLength value="0"/>
                    <xs:maxLength value="256"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <xs:element name="GROUP_NAME_LIMIT">
            <xs:simpleType>
                <xs:restriction base="xs:integer">
                    <xs:minInclusive value="1"/>
                    <xs:maxInclusive value="1000"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:element>
```

```
<xs:element name="INTEGRITY_CHECK_OBJECT_TYPES">
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:minLength value="1"/>
            <xs:maxLength value="15"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="DIGEST_HASH">
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:enumeration value="MD5" />
            <xs:enumeration value="SHA-1" />
            <xs:enumeration value="SHA-256" />
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="PERMISSION_MONITOR">
    <xs:simpleType>
        <xs:restriction base="xs:boolean">
            <xs:pattern value="true"/>
            <xs:pattern value="false"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="PATH_TYPE">
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:enumeration value="Use Registry key" />
            <xs:enumeration value="Use file search" />
            <xs:enumeration value="Use file path" />
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="DATA_TYPE">
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:enumeration value="Boolean" />
            <xs:enumeration value="Integer" />
            <xs:enumeration value="String" />
            <xs:enumeration value="String List" />
            <xs:enumeration value="Line List" />
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="DESCRIPTION">
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:minLength value="1"/>
            <xs:maxLength value="1000"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="EVALUATE_AS_STRING" default="0">
    <xs:simpleType>
```

```
            <xs:restriction base="xs:integer">
                <xs:enumeration value="0" />
                <xs:enumeration value="1" />
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <xs:element name="TECHNOLOGY_LIST">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="TECHNOLOGY" maxOccurs="unbounded" />
            </xs:sequence>
            <xs:attribute name="total" use="required" type="xs:integer" />
        </xs:complexType>
    </xs:element>

    <xs:element name="TECHNOLOGY">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="ID" maxOccurs="1"/>
                <xs:element ref="TECH_NAME" maxOccurs="1" />
                <xs:element ref="RATIONALE" maxOccurs="1" />
                <xs:element ref="REMEDIATION" minOccurs="0" maxOccurs="1" />
                <xs:element ref="DATAPOINT" minOccurs="0" maxOccurs="1" />
                <xs:element ref="USE_SCAN_VALUE" minOccurs="0" maxOccurs="1" />
                <xs:element ref="DB_QUERY" minOccurs="0" maxOccurs="1" />
                <xs:element ref="DESCRIPTION" minOccurs="0" maxOccurs="1" />
            </xs:sequence>
        </xs:complexType>
    </xs:element>

    <xs:element name="TECH_NAME">
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:minLength value="0"/>
                <xs:maxLength value="64"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <xs:element name="RATIONALE">
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:minLength value="1"/>
                <xs:maxLength value="4000"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <xs:element name="REMEDIATION">
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:minLength value="0"/>
                <xs:maxLength value="4000"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <xs:element name="DATAPOINT">
        <xs:complexType>
            <xs:sequence>
```

```
            <xs:element ref="CARDINALITY" minOccurs="0" maxOccurs="1" />
            <xs:element ref="OPERATOR" minOccurs="0" maxOccurs="1" />
            <xs:element ref="DEFAULT_VALUES" maxOccurs="1" />
        </xs:sequence>
    </xs:complexType>
</xs:element>

<xs:element name="USE_SCAN_VALUE" default="0">
    <xs:simpleType>
        <xs:restriction base="xs:integer">
            <xs:enumeration value="0" />
            <xs:enumeration value="1" />
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="CARDINALITY">
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:enumeration value="match any" />
            <xs:enumeration value="match all" />
            <xs:enumeration value="match none" />
            <xs:enumeration value="empty" />
            <xs:enumeration value="not empty" />
            <xs:enumeration value="contains" />
            <xs:enumeration value="does not contain" />
            <xs:enumeration value="matches" />
            <xs:enumeration value="is contained in" />
            <xs:enumeration value="intersect" />
            <xs:enumeration value="no cd" />
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="OPERATOR">
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:enumeration value="ge" />
            <xs:enumeration value="gt" />
            <xs:enumeration value="le" />
            <xs:enumeration value="lt" />
            <xs:enumeration value="ne" />
            <xs:enumeration value="eq" />
            <xs:enumeration value="in" />
            <xs:enumeration value="range" />
            <xs:enumeration value="re" />
            <xs:enumeration value="xre" />
            <xs:enumeration value="xeq" />
            <xs:enumeration value="no op" />
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="DEFAULT_VALUES">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="DEFAULT_VALUE" maxOccurs="unbounded" />
        </xs:sequence>
        <xs:attribute name="total" use="required" type="xs:integer" />
    </xs:complexType>
</xs:element>
```

```
<xs:element name="DEFAULT_VALUE">
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:minLength value="0"/>
            <xs:maxLength value="4000"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="DB_QUERY">
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:minLength value="0"/>
            <xs:maxLength value="32000"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="REFERENCE_LIST">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="REFERENCE" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
</xs:element>

<xs:element name="REFERENCE">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="REF_DESCRIPTION" minOccurs="0" maxOccurs="1" />
            <xs:element ref="URL" minOccurs="0" maxOccurs="1" />
        </xs:sequence>
    </xs:complexType>
</xs:element>

<xs:element name="REF_DESCRIPTION">
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:minLength value="0"/>
            <xs:maxLength value="2000"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="URL">
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:minLength value="0"/>
            <xs:maxLength value="500"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:simpleType name="yesOrNo">
    <xs:restriction base="xs:token">
        <xs:enumeration value="Yes"/>
        <xs:enumeration value="No"/>
    </xs:restriction>
</xs:simpleType>
```

```
</xs:schema>
```