GFI LanGuard 12
Scan Results Database Structure

Table of Contents

Physical Design Summary

This document describes the structure of the "scan results" database.

Apart from scan results, this DB also contains Computer, Computer Group, Computer Overview, Computer and Computer Group Settings, Attributes, and other things which are configurable per computer such as ScanProfileOverrides, Agent, Relay, Data Sync etc.

Module Development

Data Services Tier

This document describes the structure of the Scan Results.

Why is the Scan Result database needed?

The product's security scanner results, deployment results, computer, agent information etc. are stored in a database. The scan data may be stored in an MS SQL Server database or an MS Access database. For Microsoft Access, GFI LanGuard does not need any additional software to be installed on the target system.

The database to use (MSSQL server instance, MSSQL DB name) can be set or changed during the installation wizard, or in the product, from Database Maintenance Options.

We use the same database structure for Agent, Main or Central Management Server.

The data layer is used for two reasons:

- A part of the communication between operational modules (modules that gather data like: opened ports, list of users etc.) and user interface is made through the database. This is necessary considering the large amount of data that the operational modules may gather during scans performed on a large amount of machines.
- The saved scan data can be used to create reports at a later time.
- Configurations and overviews which are per computer or per computer group.

Scan Results database diagram

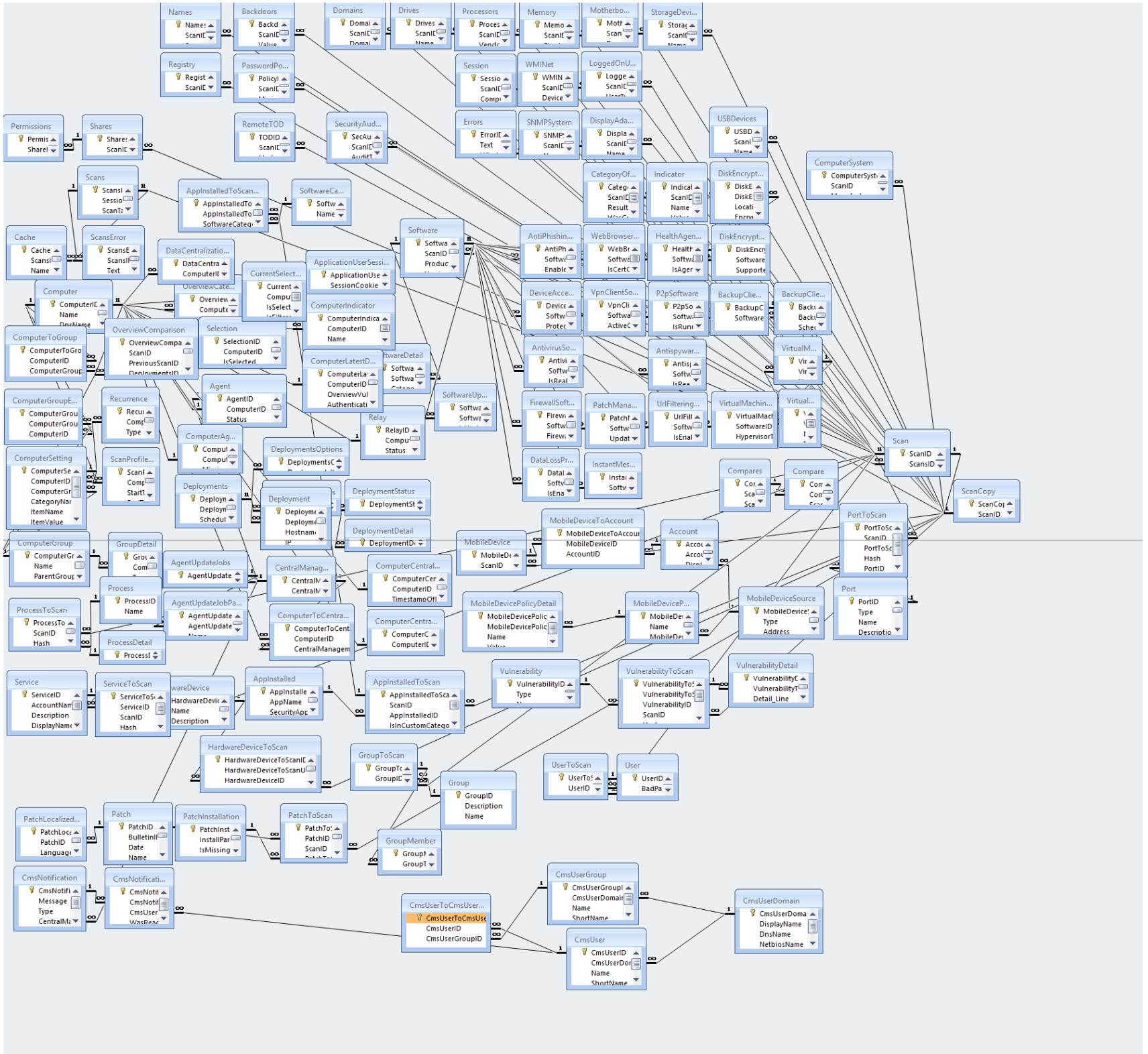
Names
Backdoors
Domains
Drives
Processors
Memory
Motherbo...
StorageDevi...
Registry
PasswordPo...
Session
WMINet
LoggedOnU...
Permissions
Shares
RemoteTOD
SecurityAud...
Errors
SNMPSystem
DisplayAda...
USBDevices
ComputerSystem
Scans
AppInstalledToScan...
SoftwareCa...
CategoryOf...
Indicator
DiskEncrypt...
Cache
ScansError
DataCentralizatio...
Software
AntiPhishin...
WebBrowser...
HealthAgen...
DiskEncrypt...
Computer
CurrentSelect...
ApplicationUserSessi...
ComputerIndicator
DeviceAcce...
VpnClientSo...
P2pSoftware
BackupClie...
BackupClie...
ComputerToGroup
OverviewComparison
Selection
ComputerLatestD...
AntivirusSo...
Antispywar...
VirtualM...
Agent
SoftwareUp...
FirewallSoft...
PatchMana...
UrlFiltering...
VirtualMachin...
Virtual...
ComputerGroupE...
Recurrence
Relay
DataLossPr...
InstantMes...
Scan
ComputerSetting
ScanProfile...
ComputerAg...
DeploymentsOptions
Compares
Compare
ScanCopy
Deployments
Deployment
DeploymentStatus
DeploymentDetail
PortToScan
ComputerGroup
GroupDetail
MobileDeviceToAccount
MobileDevice
Account
AgentUpdateJobs
CentralManag...
ComputerCentral...
Process
AgentUpdateJobPa...
MobileDevicePolicyDetail
MobileDeviceP...
MobileDeviceSource
Port
ProcessToScan
ComputerToCentra...
ProcessDetail
Service
ServiceToScan
AppInstalled
AppInstalledToScan
Vulnerability
VulnerabilityToScan
VulnerabilityDetail
HardwareDeviceToScan
GroupToScan
UserToScan
User
Group
Patch
PatchLocalized...
PatchInstallation
PatchToScan
GroupMember
CmsNotification
CmsNotificati...
CmsUserToCmsUser...
CmsUserGroup
CmsUserDomain
CmsUser

Figure 1 Relationships in the scan results DB

Figure 1 shows the diagram of the Scan Results Database. The root of the table hierarchy are tables:
* Scans - for scan results. Note that table Scan has a table ScanCopy. Each row in table Scan should have a corresponding row in table ScanCopy.
* Computer - for Computer overviews, Computer configurations, per Computer data (such as data centralization status).
* ComputerGroup - for ComputerGroup configurations, per ComputerGroup.

Most of the scan results categories are kept in a single table (for instance information about users is kept in a single table: ***Users***). Still, there are a few categories of scan results that are split in more tables.

Detailed explanation of database tables

Scans

Each record of this table corresponds to a **security scan session**. A security scan session can contain scan results from more scanned computers. Scan results for a computer is stored in a record in table.

Fields

Field Name	Type	Description
ScansID	Int	PK
ScanTarget	nvarchar[255]	Contains the target of the current scan. It may contain a single machine name: “PC1”, an IPs range: “192.168.100.1-192.168.100.255”, or a file name: “file:machines.txt”, as it is specified in the user interface.
Session	nvarchar[255]	A string that uniquely identifies a scan. Currently limited to 0-2147483647.
Profile	nvarchar[255]	LNSS generates a string that uniquely identifies a scan.
CreatedOn	Datetime	The date and the time when the scan was started.
ReadOnly	Int	This fiels is set to 0 by default. When set to 1, database maintenance module will not delete the scan data even if the database maintenance settings say that this scan should be deleted.
ScansEnded	Int	Field is 0 if the scan is not ended or to 1 if the scan completed. The field may have the 0 value when the scan is still in progress or was interrupted by the user.
ComputerProfilesEnabled	Int	Specifies if the current scan has computer profiles enabled. Value 1 means enabled, and 0 meanes disabled.
ScanDuration	Int	Time in seconds it took to scan the computer(s).
ScheduledScan	Int	Default 0. 0 – Scan was started by the user (e.g. from StartScanUI, SecurityScannerUI etc.) 1 – Scan was scheduled.
ScannedItemsCount	Int	Default 0. Represents the number of items processed during the scan: *applications installed *users, groups, services, processes gathered *ports that were scanned *vulnerability checks which were performed *patches that were checked to see if they are installed etc.
AutoremediationEnabled_MissingPatches	Int	Default 0. 0 – Otherwise 1 – The scan session is scheduled and has automatic remediation options for installing missing patches.
AutoremediationEnabled_MissingServicePacks	Int	Default 0. 0 – Otherwise 1 – The scan session is scheduled and has automatic

		remediation options for installing missing service packs.
AutoremediationEnabled_UninstallApplications	Int	Default 0. 0 – Otherwise 1 – The scan session is scheduled and has automatic remediation options for uninstalling applications (which are unauthorized and validated).
AgentScan	Int	Default 0. 0 – The scan is not an agent style scan, it is a classical scan. 1 – The scan was an agent style scan run based on the agent's recurrence settings. 2 – The scan was an agent style scan performed on demand.
Iid	nvarchar[255]	The installation ID of the product that ordered the scan session.
Uid	nvarchar[255]	A string that uniquely identifies a scan. E.g. `27241DBB-0F6F-4F32-9CAA-1EF165F278A3`.
ProductInstallLanguage	Int	Language code for installed Languard (main or agent) instance.

Scan

Each record of this table corresponds to a computer which was scanned as part of a security scan. The scan to which the machine belongs is the foreign key *ScansID*, which links the table with the primary key **ScansID** from table ***Scans***.

Fields

Field Name	Type	Description
ScanID	Autonumber	PK
BDC	nvarchar[255]	Contains the Backup Domain Controller. The field is empty if the scanned machine is not joined to a domain or the BDC could not be retrieved.
Domain	nvarchar[255]	Domain that the machine is joined to.
HostName	nvarchar[255]	Machine's name. In most cases this is the NETBIOS name.
IP	nvarchar[255]	Machine's IP.
Information	Int	1 – if target machine replied to ICMP Information request, 0 otherwise
IsWindows	Int	• -1 – N/A (i.e. we do not know if the remote host is windows, target does not respond to ping) • 1 – if target machine is Windows • 0 – otherwise
Kernel	nvarchar[50]	The name of the Kernel in case of a Linux/Unix machine.
Language	nvarchar[255]	The language identifier of the OS on the scanned machine. For instance for English this field's value is "0049".
LanMan	nvarchar[255]	The Network Manager on this machine.
MAC	nvarchar[255]	The MAC address of the network card.
MACVendor	nvarchar[255]	The network card manufacturer.
Mask	nvarchar[255]	The network mask. This is only retrieved if the scanned machine has Windows 98 installed. On other OSes this field is empty.
NMB	Int	The field value is 1 if NETBios is running, otherwise the field value is 0.
OS	nvarchar[255]	Contains the operating system, i.e. "Windows XP".
PDC	nvarchar[255]	Contains the Primary Domain Controller. The field is empty if the scanned machine is not joined to a domain or the PDC could not be retrieved.
RealTTL	Int	Time to live in the packets received from the scanned host.
RefID	Int	Points to the next row from the Scan table (as odered by column CreatedOn from table Scans) which contains scan results from the same remote computer/host. I.e. If

		we scan a computer 3 times, the first scan will point to the second and the second will point to the third and last; the last scan will have a RefID equal to NULL. Has the same possible values as ScanID column, plus it allows NULL.
RefData	nvarchar[255]	Contains the string "<RefID>_<HostName>" in encoded format.
REG	Int	
RespondedToPing	Int	The field is 1 if the scanned machine responded to ping, 0 otherwise.
ScanEnded	Int	The field is initially set to 0 when the current host's scan begins. When the scan of the current host ends, this is set to 1. If the scan was interrupted before completion the field's value remains 0.
ScansID	Int	FK
SecAuditRetrieved	Int	1 if the security audit policy was successfully retrieved. The field value is 0 if the policy could not be retrieved.
ServicesNextRunLevel	Int	The next services run level when scaning a Linux/Unix machine.
ServiceRunLevel	Int	The current services run level when scaning a Linux/Unix machine.
ServPack	nvarchar[50]	The operating system installed service pack.
SMB	Int	1 if Samba is available, 0 otherwise.
SMBHostName	nvarchar[255]	The machine name as it is contained in the Samba packets.
SNMP	Int	1 if SNMP is running on the scanned machine, 0 otherwise.
TimeStamp	Int	1 if the machine responded to the ICMP timestamp request, 0 otherwise.
TTL	Int	Maximum time to live in the packets received from the scanned host.
Usage	nvarchar[255]	The usage of the scanned machine, for instance "Workstation". Note: do not translate.
UserName	nvarchar[255]	The currently logged on user.
VulnerabilityLevel	Int	0 - not defined. 1-10 increasing vulnerability levels. This value is computed per computer and represents an overview of the vulnerabilities found on the computer.
WWW	nvarchar[50]	The web server type and version, for instance "Microsoft-IIS/5.1".
WWWKind	nvarchar[50]	Contains the web server type; possible values: "IIS", "apache" and "other". Note: do not translate.
ComputerStatus_ID	Int	Foreign Key. The ID of the computer. Foreign key to table ComputersStatus.
VulnLevel_VulnAssessment	Int	Vulnerability level resulted from this scan session. The vulnerability level for the computer calculated by the vulnerability assessment component of the application.
VulnLevel_PatchMngmt	Int	Vulnerability level resulted from this scan session. The vulnerability level for the computer calculated by the patch management component of the application.
VulnLevel_NetworkAudit	Int	Vulnerability level resulted from this scan session. The vulnerability level for the computer calculated by the network & software audit component of the application.
VirtualizationTechnology	nvarchar[255]	Possible values "VMware", "Microsoft Virtual PC" or empty. Empty or NULL value means that the scanned machine is not a guest OS inside a virtual machine. If the value is a non empty string, then the scanned machine is a guest OS running inside a virtual machine. Currently we support only the mentioned virtualization

		technologies. Note: do not translate.
ScanDuration	Int	Time in seconds it took to scan a single computer.
OSSerialNumber	nvarchar[255]	Serial number for the Operating System (e.g. for Microsoft Windows).
ComputerID	Number (FK)	The ID of the computer. FK to table Computer.
OrganizationalUnit	nvarchar[255]	Active Directory Organizational Unit (OU) of the current computer.
IsVirtualMachine	Int	Possible values: 0 – N/A, 1 – the scanned machine is a virtual machine, 2 –the scanned machine is not a virtual machine
StartTime	Datetime	Time when scanning this computer started.
EndTine	DateTime	Time when scanning this computer ended.
DnsName	nvarchar[255]	DNS fully qualified computer name.
Hardware	nvarchar[255]	The name of the hardware of the machine.
TimezoneOffset	Int	Timezone offset in seconds.
ComputerUniqueID	nvarchar[255]	Computer unique identifier

ScanCopy

Contains a field which is a unique index, with a one to one relationship with field ScanID from table Scan. It is needed in order to overcome the 32 indexes limit on table Scan.
Table Scan has a table ScanCopy. Each row in table Scan should have a corresponding row in table ScanCopy.

More details about this limitation of Microsoft Office Access are available here.

Fields

Field Name	Type	Description
ScanCopyID	Autonumber	PK
ScanID	Number	Default 0. Unique index. One to one relationship with field ScanID from table Scan.

Port

Each record of this table corresponds to an open port. It is a 3NF parent table.

Fields

Field Name	Type	Description
PortID	Int	PK
Type	Int	0 if this is a TCP port and 1 if it is an UDP port.
Name	Int	This field contains the open port number.
Description	nvarchar[255]	A text that describes the standard service that it is usually running on the specified port number.
IsTrojan	Int	1 if the current port is known to be used by a Trojan, 0 otherwise.
Lines	Memo	This field contains the lines from the port banner (the text that the server service running on this port is responding with after the connection is initiated). The lines are separated with CR LF characters in this field.
Service	nvarchar[255]	The name of the service that has opened the port.
ProcessID	Number	Process ID of the process that listens on that port. Possible value: -1 – could not get the process ID.
ProcessName	NVarchar[255]	Name of the process that listens on that port. E.g. `svchost.exe`.
ProcessPath	NVarchar[255]	Full path of the executable of the process that listens on that port. E.g. `C:\WINDOWS\system32\svchost.exe`.
ProcessCommandLine	Memo	Command line of the process that listens on that port.

		E.g. `C:\Windows\system32\svchost.exe -k DcomLaunch`.

PortToScan

A table is needed in order to link the 3NF parent table with the Scan table.

Process and ProcessDetail

A running process on a computer

Fields

Field Name	Type	Description
ProcessesID	Int	PK
Name	Int	The running process name.
CommandLine	nvarchar[255]	The command line used to start the process.
Domain	nvarchar[255]	The domain name under which the process is running.
HandleCount	Int	The count of the handles to this process.
Path	nvarchar[255]	Path to the executable file of the process.
PID	Int	Global process identifier that can be used to identify the process.
PPID	Int	Unique identifier of the process that created this process.
Priority	Int	Scheduling priority of the process within the operating system.
ThreadCount	Int	Number of the active threads in this process.
UserName	nvarchar[255]	The user name under which the process is running.
CommandLine	nvarchar[255]	The command line used to start the process.

ProcessToScan

A table is needed in order to link the 3NF parent table with the Scan table.

Service

Windows services, *nix init services, systemd services, MAC OS X services and other types of OS services.

Fields

Field Name	Type	Description
ServiceID	Int	PK
Name	nvarchar[255]	The service name.
DisplayName	nvarchar[255]	Service's display name.
Description	Memo	Service's description.
Status	Int	This is the service status. Possible values: 1 – service is stopped 4 – service is running
Start	Int	This is the service startup type. Possible values: 2 – Automatic startup 3 – Manual 4 – Disabled
AccountName	nvarchar[255]	The user account under which the service is running.
SysVRunlevels	nvarchar[50]	The list of Linux/ SysV init runlevels in which the current service is being automatically started by SysV init daemon. Further details available here. String containing runlevels separated by commas.

ServiceToScan

A table is needed in order to link the 3NF parent table with the Scan table.

Field Name	Type	Description
ServiceToScanID	Int	PK
ScanID	Int	FK
ServiceID	Int	FK

Session

Sessions which are open on a computer.

Fields

Field Name	Type	Description
SessionID	Int	PK
ScanID	Int	FK
ComputerName	nvarchar[255]	The computer that established the session.
ClientType	nvarchar[255]	The type of client that established the session (LAN Manager). Note: do not translate.
ConnectionTime	Int	The number of seconds the session has been active.
IdleTime	Int	The number of seconds the session has been idle.
OpenFiles	Int	The number of files, devices, and pipes opened during the session.
Transport	nvarchar[255]	The name of the transport that the client is using to communicate with the server. Note: do not translate.
UserFlags	Int	Specifies a value that describes how the user established the session.
UserName	nvarchar[255]	The name of the user who established the session.
ComputerID	bigint	Not zero if part of Overview for that Computer.
SessionUid	nvarchar[36] uniqueidentifier	Unique row identifier.
Hash	nvarchar(40)	Content hash.

User

A computer user.
Fields

Field Name	Type	Description
UserID	Int	PK
FullName	nvarchar[255]	User's full name.
Privilege	nvarchar[255]	User's privilege; for instance: "Guest", "Administrator (*)" Note: do not translate.
Flags	nvarchar[255]	User's account flags; possible values that are enumerated in a comma separated list are: - ACCOUNT_DISABLED - PASSWORD_NOT_REQUIRED - PASSWORD_CANNOT_BE_CHANGED Note: do not translate.
Homedir	nvarchar[255]	User's home directory
Comment	nvarchar[255]	User's account comment.
UserComment	nvarchar[25	User's account comment.

	5]	
ScriptPath	nvarchar[255]	Path to the script that is executed when the user logs on.
Workstations	nvarchar[255]	The workstations from which the user is allowed to log on (this only applies to a domain user).
LastLogon	nvarchar[255]	The last date and time when the user logged on. Possible values: “Never” or the date and the time in the format: “01 Apr 2004, 10:22:03” Note: do not translate.
NoLogons	Int	Number of logons that the user made.
BadPasswordCount	Int	Number of times the user entered wrong passwords.
Name	nvarchar[255]	User account’s name.
Enabled	Int	1 – if user account is enabled, 0 – if account is disabled.
LoginShell	nvarchar[255]	The shell used to log-in the system.
PasswordChangedTimestamp	Datetime	Date when password was last changed for user.

UserToScan

Each record of this table represents a link between a user and a scan.

Field Name	Type	Description
UserToScanID	Int	PK
UserID	Int	Id of the user.
ScanID	Int	Id of the scan.
ComputerID	bigint	Not zero if part of Overview for that Computer.
UserToScanUid	nvarchar[36] uniqueidentifier	Unique row identifier.
Hash	nvarchar(40)	Content hash.

Group

Each record form this table corresponds to a group.

Fields

Field Name	Type	Description
GroupID	Int	PK
GroupToScanID	Int	FK
Name	nvarchar[255]	Group name.
Description	nvarchar[255]	Group description.

GroupToScan

Table with links of the groups to scans.

Field Name	Type	Description
GroupToScanID	Int	PK
GroupID	Int	Id of a group from Group table.
ScanID	Int	Id of the scan that group corresponds to.
ComputerID	bigint	Not zero if part of Overview for that Computer.
GroupToScanUid	nvarchar[36] uniqueidentifier	Unique row identifier.

Hash	nvarchar(40)	Content hash.

GroupMember

Each record form this table corresponds to a group member.
Fields

Field Name	Type	Description
GroupMemberID	Int	PK
GroupToScanId	Int	FK
Name	nvarchar[255]	User name.
Type	Int	Specifies the account type of the member. The following values are valid. 1 – (SidTypeUser): The account is a user account. 2 – (SidTypeGroup): The account is a global group account. 5 – (SidTypeWellKnownGroup): The account is a well-known group account (such as Everyone). 6 – (SidTypeDeletedAccount): The account has been deleted. 8 – (SidTypeUnknown): The account type cannot be determined.

Drives

Each record form this table corresponds to a hard drive on a specific machine (in a specific scan). The machine on which the drive is located is the foreign key *ScanID*, which links the table with the primary key **ScanID** from table ***Scan***.

Fields

Field Name	Type	Description
DrivesID	Int	PK
ScanID	Int	FK
Name	nvarchar[255]	Drive name, for instance “A:”, “C:” etc.
TotalSpace	nvarchar[255]	Total space on this drive.
FreeSpace	nvarchar[255]	Free space on this drive.
FileSystemType	nvarchar[255]	The type of the file system present on this drive. This field is used now for Linux scans.
ComputerID	bigint	Not zero if part of Overview for that Computer.
DrivesUid	nvarchar[36] uniqueidentifier	Unique row identifier.

Domains

The Domains table contains the trusted domains from a domain controller.

Fields

Field Name	Type	Description
DomainID	Int	PK
ScanID	Int	FK
DomainName	nvarchar[255]	Trusted domain name.
ComputerID	bigint	Not zero if part of Overview for that Computer.
DomainsUid	nvarchar[36] uniqueidentifier	Unique row identifier.
Hash	nvarchar(40)	Content hash.

Names

The Names table contains the NetBIOS names from the scanned machine.

Fields

Field Name	Type	Description
NamesID	Int	PK
ScanID	Int	FK
Serv	nvarchar[255]	NetBIOS name.
Type	nvarchar[255]	Name description.
ComputerID	bigint	Not zero if part of Overview for that Computer.
NamesUid	nvarchar[36] uniqueidentifier	Unique row identifier.
Hash	nvarchar(40)	Content hash.

SecurityAuditEvents

Each record in this table corresponds to an event that audit enabled on a machine. If an audit event does not appear in the table for a specified machine that means the audit is disabled for the event.

Fields

Field Name	Type	Description
SecAuditID	Int	PK
ScanID	Int	FK
AuditType	Int	The event that has auditing enabled. Possible values are: 0 - AUDIT_SYSTEM_FAILURE, 1 - AUDIT_SYSTEM_SUCCESS, 2 - AUDIT_LOGON_FAILURE, 3 - AUDIT_LOGON_SUCCESS, 4 - AUDIT_OBJECT_ACCESS_FAILURE, 5 - AUDIT_OBJECT_ACCESS_SUCCESS, 6 - AUDIT_PRIVILEGE_USE_FAILURE, 7 - AUDIT_PRIVILEGE_USE_SUCCESS, 8 - AUDIT_DETAILED_TRACKING_FAILURE, 9 - AUDIT_DETAILED_TRACKING_SUCCESS, 10 - AUDIT_POLICY_CHANGE_FAILURE, 11 - AUDIT_POLICY_CHANGE_SUCCESS, 12 - AUDIT_ACCOUNT_MANAGEMENT_FAILURE, 13 - AUDIT_ACCOUNT_MANAGEMENT_SUCCESS, 14 - AUDIT_DIRECTORY_SERVICE_ACCESS_FAILURE, 15 - AUDIT_DIRECTORY_SERVICE_ACCESS_SUCCESS, 16 - AUDIT_ACCOUNT_LOGON_FAILURE, 17 - AUDIT_ACCOUNT_LOGON_SUCCESS
ComputerID	bigint	Not zero if part of Overview for that Computer.
SecurityAuditEventsUid	nvarchar[36] uniqueidentifier	Unique row identifier.
Hash	nvarchar(40)	Content hash.

Registry

The Registry table contains some registry keys from the scanned machine.

Fields

Field Name	Type	Description
RegistryID	Int	PK
ScanID	Int	FK

NodeName	nvarchar[255]	Contains the node name specified in toolcfg_regparams.xml. Empty if the node is “Main”.
RegEntry	nvarchar[255]	Contains the registry key name and its value separated by “ : “.
ComputerID	bigint	Not zero if part of Overview for that Computer.
RegistryUid	nvarchar[36] uniqueidentifier	Unique row identifier.
Hash	nvarchar(40)	Content hash.

PasswordPolicy

This table contains data about the password policy from the local security policy from the scanned machine. One record corresponds to one scanned machine.

Fields

Field Name	Type	Description
PolicyID	Int	PK
ScanID	Int	FK
ForceLogoff	nvarchar[255]	Specifies, in seconds, the amount of time between the end of the valid logon time and the time when the user is forced to log off the network. A value of TIMEQ_FOREVER (-1) indicates that the user is never forced to log off. A value of zero indicates that the user will be forced to log off immediately when the valid logon time expires.
MaximumPasswordAge	nvarchar[255]	Specifies, in seconds, the maximum allowable password age. A value of TIMEQ_FOREVER (-1) indicates that the password never expires. The minimum valid value for this element is ONE_DAY (01*24*3600). The value specified must be greater than or equal to the value for the MinimumPasswordAge member
MinimumPasswordAge	nvarchar[255]	Specifies the minimum number of seconds that can elapse between the time a password changes and when it can be changed again. A value of zero indicates that no delay is required between password updates. The value specified must be less than or equal to the value for the MaximumPasswordAge member.
MinimumPasswordLength	nvarchar[255]	Specifies the minimum allowable password length. Valid values for this element are zero through PWLEN (256).
PasswordHistory	nvarchar[255]	Specifies the length of password history maintained. A new password cannot match any of the previous PasswordHistory passwords. Valid values for this element are zero through DEF_MAX_PWHIST (8).
ComputerID	bigint	Not zero if part of Overview for that Computer.
PasswordPolicyUid	nvarchar[36] uniqueidentifier	Unique row identifier.
Hash	nvarchar(40)	Content hash.

PatchToScan

This table contains the relation with the tables Scan, Patch and PatchInstallation.

Fields

PatchToScanID	AutoNumber	
PatchID	Number	
ScanID	Number	

PatchToScanUid	Text	
Hash	Text	
ComputerID	bigint	Not zero if part of Overview for that Computer.
PatchCategory	Number	
PatchInstallationID	Number	
IsMajorVersionUpgrade	Number	Possible values: 0 - N/A, 1 - is major version upgrade.

Note: All Memo fields are of type ntext on MSSQL Server. This means we need to use `substr(<FieldName>, 0, 4000)` in order to use this field in indexes, sort operations and joins.

Patch

This table contains all the patches that were detected on any machine in the network with the fields that are static and that are explicitly defining a Patch. This is a 3NF parent table/dictionary. It is linked to PatchToScan table by the PatchID field.

Fields

Field Name	Type	Description
PatchID	AutoNumber	PK
BulletinID	Text	This is the name of the MS security bulletin that contains the update.
Date	Text	Specifies the date when the update was released.
Name	Text	Is the KB number of the update (aka QNumber in the old system).
Title	Text	This is the title of the update.
Severity	Text	
AppliesToCategory	Text	
UpdateType	Text	
Url	Memo	The URL address where the update is described.
Supersedindex	Memo	
FileDigest	Memo	Contains the update file digest (hash)
FileName	Memo	This is the name of the file.
FileSize	Memo	Specifies the size of the file as in the xml file.
FileURL	Memo	The URL address where the update can be downloaded from.
MSIPatchGUID	Text	This is MSIPatchGUID for Office updates as in the xml file
DigestAlgorithm	Text	Hash on this table used to quickly identify the patches.
References	Memo	Links to the associated Microsoft bulletin.
Vendor	Text	Patch's vendor
Product	Text	Product a patch applies to
IsForMobileDevice	Number	Possible values: 0 - N/A, 1 - is mobile device update (operating system update or application update).
OSFamily	Text	Possible values: Windows, Mac, Windows Mobile, Android, iOS, BlackBerry, Symbian, etc.
AppliesTo	Memo	List of products the patch applies to.(i.e. "Windows Vista; Windows Server 2008; Windows 7")
Description	Memo	Patch description in English.

Note: All Memo fields are of type ntext on MSSQL Server. This means we need to use `substr(<FieldName>, 0, 4000)` in order to use this field in indexes, sort operations and joins.

PatchInstallation

This table contains all the patches scanning detection information that were detected on any machine in the network with the fields that are static and that are explicitly defining a patch installation attribute. This is a 3NF parent table/dictionary. It is linked to PatchToScan table by the PatchInstallationID field.

Fields

Field Name	Type	Description
PatchInstallationID	AutoNumber	
InstallParameters	Memo	
IsMissing	Number	
UninstallCommand	Memo	
IsUninstallable	Number	
IsMajorVersionUpgrade	Number	Possible values: 0 - N/A, 1 - is major version upgrade.
RequiresLicenseKeyUpdate	Number	Reserved for future use.
IsSecurityUpdate	Number	Possible values: 0 - N/A, 1 - is security update.
IsDeployable	Number	Possible values: 0 - N/A, 1 - we can remediate the missing update by deploying the update.

Note: All Memo fields are of type ntext on MSSQL Server. This means we need to use `substr(<FieldName>, 0, 4000)` in order to use this field in indexes, sort operations and joins.

SNMPSystem

The SNMPSystem table contains SNMP entries from the scanned machine.

Fields

Field Name	Type	Description
SNMPSystemID	Int	PK
ScanID	Int	FK
Name	nvarchar[255]	SNMP entry name.
Description	nvarchar[255]	Contains the SNMP entry value.
ComputerID	bigint	Not zero if part of Overview for that Computer.
SNMPSystemUid	nvarchar[36] uniqueidentifier	Unique row identifier.
Hash	nvarchar(40)	Content hash.

Shares

The Shares table contains share entries from the scanned machine.

Fields

Field Name	Type	Description
SharesID	Int	PK
ScanID	Int	FK
Name	nvarchar[255]	Share name.
Remark	nvarchar[255]	Share comment.
Path	nvarchar[255]	Path to the shared resource on the scanned machine.
PrinterShare	Int	Has the value 1 if the shared resource is a printer, 0 otherwise.
Passworded	Int	Has the value 1 if the shared resource is password protected 0 otherwise.
SDIncluded	Int	Possible values: 1 or 3 if the shared resource has permissions (on Windows NT or greater) or has password (on Windows 9x or Samba server on Unix/Linux), 0 or 2 otherwise. Note: value 1 is equivalent to value 3; value 0 is equivalent to value 2.
AppliesTo	Memo	List of products the patch applies to.(i.e. "Windows Vista; Windows Server 2008; Windows 7")

ComputerID	bigint	Not zero if part of Overview for that Computer.
SharesUid	nvarchar[36] uniqueidentifier	Unique row identifier.
Hash	nvarchar(40)	Content hash.

Permissions

The Permissions table contains share permissions entries from the scanned machine.

Fields

Field Name	Type	Description
PermissionID	Int	PK
ShareID	Int	FK
Type	nvarchar[255]	Permission type. Possible values: “Allow”, “Deny”. Note: do not translate.
UserName	nvarchar[255]	User account for which the permission apply.
Verb	nvarchar[255]	This the permission. Values: “Read”, “Full Control” etc. Note: do not translate.
NTFS	Int	Possible values: 0 - It’s a share permission. 1 - It’s a path NTFS permission.
Flags	Text	Text that describes where the permissions apply. Examples: “Apply to subfolders and files only” “Apply to this folder, subfolders and files” “Apply to this folder and subfolders” Note: do not translate.

RemoteTOD

The RemoteTOD table contains the Remote Time of Day from the scanned machine.

Fields

Field Name	Type	Description
TODID	Int	PK
ScanID	Int	FK
ComputerID	bigint	Not zero if part of Overview for that Computer.
RemoteTODUid	nvarchar[36] uniqueidentifier	Unique row identifier.
Hash	nvarchar(40)	Content hash.
StartupTimestamp	Datetime	Date when computer was powered on.

Errors

The various security scanner modules log errors (e.g. “Could not connect to remote registry”) to this table.

Fields

Field Name	Type	Description
ErrorID	Int	PK
ScanID	Int	FK
Text	nvarchar[255]	Error text.
WindowsErrCode	nvarchar[255]	Windows error code. Note: do not translate.
Context	nvarchar[25	Not used yet.

	5]	
Timestamp	Date/Time	The date and time when the error occurred.

HardwareDevice

Other types of hardware devices.

Fields

Field Name	Type	Description
HardwareDeviceID	Int	PK
Name	nvarchar[255]	The name of the hardware device as is available in DEVMGR (e.g. for device “ACPI Fixed Feature Button”, the text is taken from registry `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\ACPI\FixedButton\2&daba3ff&0\DeviceDesc`. The text could also be taken from FriendlyName registry value (e.g. for device “Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GHz”, from registry value `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\ACPI\GenuineIntel_-_EM64T_Family_6_Model_15\_0\FriendlyName`).
Description	nvarchar[255]	Description of the hardware device. Always taken from registry value `DeviceDesc`.
Manufacturer	nvarchar[255]	Device manufacturer. Mainly taken from registry value `Mfg`. E.g. . for device “Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GHz”, from registry value `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\ACPI\GenuineIntel_-_EM64T_Family_6_Model_15\_0\Mfg`.
ClassGuid	nvarchar[255]	Specifies the device class GUID, formatted as shown here: `{nnnnnnnn-nnnn-nnnn-nnnn-nnnnnnnnnnnn}`, where each n is a hexadecimal digit. Defined in registry value ClassGUID, e.g. for device “Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GHz”, from registry value `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\ACPI\GenuineIntel_-_EM64T_Family_6_Model_15\_0\ClassGUID`.
WhiteStatus	Int	This field tells if the device is configured as allowed in the application. Values: 0 – device is not in the white list nor in the blacklist 1 – device is in the white list 1 – device is in the blacklist
Vendor	nvarchar[255]	N/A
SerialNumber	Nvarchar[255]	Serial number of device, e.g. “WD-WMA6S1451914”.

Note: the structure of the above described table is the same as the structure of the table `USBDevices`.

HardwareDeviceToScan

Contains the relation of the hardware devices with scans.

Fields

Field Name	Type	Description
HardwareDeviceToScanID	Int	PK
HardwareDeviceID	Int	FK
ScanID	Int	FK
ComputerID	bigint	Not zero if part of Overview for that Computer.

HardwareDeviceToScanUid	nvarchar[36] uniqueidentifier	Unique row identifier.
Hash	nvarchar(40)	Content hash.

Motherboards

Contains details about the motherboard (base board) of the computer.

Fields

Field Name	Type	Description
MotherboardID	Int	PK
ScanID	Int	FK
BoardProductName	Nvarchar[255]	Taken from registry value `HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\BIOS\BaseBoardProduct`. E.g. `P5K`.
BoardManufacturer	Nvarchar[255]	Taken from registry value `HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\BIOS\BaseBoardManufacturer`. E.g. `ASUSTeK Computer INC`.
BoardVersion	Nvarchar[255]	Taken from registry value `HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\BIOS\BaseBoardVersion`. E.g. `Rev 1.xx`.
SerialNumber	Nvarchar[255]	Serial number of device, e.g. “WD-WMA6S1451914”.
BiosName	Nvarchar[255]	Taken from WMI `Win32_BIOS.Name`.
BiosVendor	Nvarchar[255]	Taken from registry value `HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\BIOS\BIOSVendor`. E.g. `American Megatrends Inc.`
BiosVersion	Nvarchar[255]	Taken from registry value `HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\BIOS\BIOSVersion`. E.g. `0704`.
BiosReleaseDate	Nvarchar[255]	Taken from registry value `HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\BIOS\BIOSReleaseDate`. E.g. `10/30/2007`.
BiosSerialNumber	Nvarchar[255]	BIOS serial number, e.g. “WD-WMA6S1451914”.
Description	Nvarchar[255]	Not used.
ComputerID	bigint	Not zero if part of Overview for that Computer.
MotherboardsUid	nvarchar[36] uniqueidentifier	Unique row identifier.
Hash	nvarchar(40)	Content hash.

StorageDevices

Contains the list of HDDs, Solid State Drives, floppy disk drives, USB storage devices etc. currently available on the scanned computer.

Fields

Field Name	Type	Description
StorageDeviceID	Int	PK
ScanID	Int	FK

Name	Nvarchar[255]	Name of storage device. E.g. `ST3250410AS`.
Description	Nvarchar[255]	N/A
Manufacturer	Nvarchar[255]	E.g. `Seagate`.
InterfaceType	Nvarchar[255]	Possible values: `IDE`, `USB`, `SCSI`. Note: do not translate.
MediaType	Int	0- N/A, format is unknown 1- Fixed hard disk media (E.g. IDE or SCSI non removable HDDs) 2- Removable media other than floppy (E.g. SD card, USB pen drive) 3- External hard disk media 4- Optical disk drive 5- Floppy disk drive
PartitionsCount	Int	The number of primary and extended partitions on the storage device for devices with PC BIOS Partition Table disk partitioning.
MountedPartitions	Nvarchar[255]	Comma separated list of Windows drives (e.g. `c:\,d:\,f:\`) or Linux mounted partitions from this storage device (e.g. `/boot,/`).
Size	Int	In MB (mebibyte, 1024^2 bytes, 1,048,576 bytes).
SerialNumber	Nvarchar[255]	Serial number of device, e.g. “WD-WMA6S1451914”.
ComputerID	bigint	Not zero if part of Overview for that Computer.
StorageDevicesUid	nvarchar[36] uniqueidentifier	Unique row identifier.
Hash	nvarchar(40)	Content hash.

DisplayAdapters

Contains the list of display adapters (GPUs etc.) present on the scanned computer.

Fields

Field Name	Type	Description
DisplayAdapterID	Int	PK
ScanID	Int	FK
Name	Nvarchar[255]	E.g. `NVIDIA GeForce 8600 GT`.
Description	Nvarchar[255]	N/A
Manufacturer	Nvarchar[255]	E.g. `NVIDIA`.
InterfaceType	Nvarchar[255]	Possible values: `PCIe`, `PCI`, `AGP`. Note: do not translate.
InstalledRam	Int	In MB (mebibyte, 1024^2 bytes, 1,048,576 bytes). E.g. `512`.
CurrentResolution	Nvarchar[255]	If possible, in the form: <HorizontalResolution> x <VerticalResolution> x <RefrashRate> Hz. E.g. 1280 x 1024 x 60 hertz.
SerialNumber	Nvarchar[255]	Serial number of device, e.g. “WD-WMA6S1451914”.
ComputerID	bigint	Not zero if part of Overview for that Computer.
DisplayAdaptersUid	nvarchar[36] uniqueidentifier	Unique row identifier.
Hash	nvarchar(40)	Content hash.

Memory

Contains information about the RAM and swap (virtual memory) from the scanned computer.

Fields

Field Name	Type	Description

MemoryID	Int	PK
ScanID	Int	FK
PhysicalMemory	Int	In MB (mebibyte, 1024^2 bytes, 1,048,576 bytes). E.g. 4000.
FreePhysicalMemory	Int	In MB (mebibyte, 1024^2 bytes, 1,048,576 bytes). E.g. 2132.
VirtualMemory	Int	In MB (mebibyte, 1024^2 bytes, 1,048,576 bytes). E.g. 787.
FreeVirtualMemory	Int	In MB (mebibyte, 1024^2 bytes, 1,048,576 bytes). E.g. 752.
ComputerID	bigint	Not zero if part of Overview for that Computer.
MemoryUid	nvarchar[36] uniqueidentifier	Unique row identifier.
Hash	nvarchar(40)	Content hash.

ComputerSystem

Contains information about scanned systems as a whole, especially for OEM systems.

Fields

Field Name	Type	Description
ComputerSystemID	Int	PK
ScanID	Int	FK
Manufacturer	nvarchar[255]	Name of the manufacturer E.g. "Apple, Inc.", "Dell Inc.".
ModelName	nvarchar[255]	Model name of the system E.g. "MacBook Air 4.2".
ModelNumber	nvarchar[255]	Model number of the system E.g. "A1369 (EMC 2392)".
SerialNumber	nvarchar[255]	Serial number of the system E.g. "C02472B7DJWR".
OsInstallDate	DateTime	Date of the OS installation.
WarrantyExpiration	DateTime	Date of warranty expiration.
FormFactor	Int	Possible values: 0 - N/A, 1 - Mobile Phone, 2 - Tablet PC
ServiceTag	nvarchar[255]	Service tag for HP or Dell computers.
ComputerID	bigint	Not zero if part of Overview for that Computer.
ComputerSystemUid	nvarchar[36] uniqueidentifier	Unique row identifier.
Hash	nvarchar(40)	Content hash.

AlertDetails

The AlertDetails contains texts lines outputted by security scanner vulnerabilities scripts. An Alert (record from table Alerts) can have none or more AlertDetails (records). An AlertDetails record is linked with an Alert through their foreign key ALERTID from table AlertDetails.

Fields

Field Name	Type	Description
ALERT_DETAILID	AutoNumber	PK
ALERTID	Int	FK
DETAIL_LINE	nvarchar[255]	Text outputted by the alert's script
DETAIL_LINE_PARENT	nvarchar[255]	Parent of this alert detail record. Alert records can be organized on multiple levels by using this field. The field contains the parent's DETAIL_LINE or is empty if it has no parent (it's on first level).
FLAGS	Int	Not used for the moment. Reserved for future use.

Backdoors

The Backdoors table contains the backdoors found on scanned machine.

Fields

Field Name	Type	Description
BackdoorsID	Int	PK
ScanID	Int	FK
Value	nvarchar[255]	Short description of the backdoor.
ComputerID	bigint	Not zero if part of Overview for that Computer.
BackdoorsUid	nvarchar[36] uniqueidentifier	Unique row identifier.
Hash	nvarchar(40)	Content hash.

Compares

The ***Compares*** and ***Compare*** tables contain temporary data to be used by reporting tools that highlight the differences between two scans.
The Compares table contains scan results compare entries. Each record represents a scan results comparison session.
Fields

Field Name	Type	Description
ComparesID	Int	PK
ScansID1	Int	Foreign key that links this compare to the first scan of the comparison.
ScansID2	Int	Foreign key that links this compare to the second scan of the comparison.
Options	Memo	An XML with the comparison options.

Compare

The ***Compares*** and ***Compare*** tables contain temporary data to be used by reporting tools that highlight the differences between two scans.

Each record in the ***Compare*** table represents a difference that was identified when comparing. The foreign key *ComparesID* links the current record with the compare from the ***Compares*** table with the primary key **ComparesID**. The foreign key *ScanID* links the current record with the machine on which the difference was identified.

Fields

Field Name	Type	Description
CompareID	Int	PK
ComparesID	Int	FK
ScanID	Int	The ScanID which represents the overview for the baseline computer. Do not read from this field.
SecondScanID	Int	The ScanID which represents the overview for a computer to compare against the baseline computer. Do not read from this field.
ResultsCategoryName	Nvarchar[255]	The category of information. E.g. "HardwareDevices".

CompareType	Int	Detailed category of information. E.g. 38 (DisplayAdapters).
		This value says what types of items were compared when the difference was identified. This field is useful to group the information in the compare report by type of data compared. Possible values:
		ctGeneralScans = -10;
		ctANewComputerHasBeenDiscovered = -2;

		ctRemediation = -1;
		ctVulnerabilityLevel = 0;
		ctGeneralHost = 1;
		ctUsers = 2;
		ctGroups = 3;
		ctTCPPorts = 4;
		ctUDPPorts = 5;
		ctServices = 6;
		ctShares = 7;
		ctTransports = 8;
		ctNames = 9;
		ctRegistry = 10;
		ctBackdoors = 11;
		ctDNSAlerts = 13;
		ctFTPAlerts = 14;
		ctHotfixes = 15;
		ctInfoAlerts = 16;
		ctMailAlerts = 17;
		ctMiscAlerts = 18;
		ctRegistryAlerts = 20;
		ctRPCAlerts = 21;
		ctRPCServices = 22;
		ctSecurityAudit = 23;
		ctMissingHotfixes = 24;
		ctServiceAlerts = 25;
		ctPasswordPolicy = 26;
		ctUsbDevices = 27;
		ctAppsInstalled = 28;
		ctUnauthorizedApplicationsAlerts = 29;
		ctSecurityProductsAlerts = 30;
		ctSoftwareAlerts = 31;
		ctWebAlerts = 32;
		ctRootkitAlerts = 33;
		ctDrives = 34;
		ctProcessors = 35;
		ctMotherboards = 36;
		ctStorageDevices = 37;
		ctDisplayAdapters = 38;
		ctMemory = 39;
		ctOtherHardwareDevices = 40;
		ctBlackListedUsbDevicesAlerts = 41;
		ctBlackListedNetworkDevicesAlerts = 42;
		ctMalwareProtectionAlerts = 43;
		ctFirewallAlerts = 44;
		ctAntispywareRecentlyDetectedThreat = 45;
		ctAntivirusRecentlyDetectedThreat = 46;

Title	Nvarchar[255]	Short description of the change. E.g. "Removed display adapter".
Text	Ntext	Complete information about this change. E.g. "Device 'Samsung SyncMaster 12-4581' has been removed."
ScanIDWithResults	Int	The ScanID which actually has the results which were compared for the baseline computer. Do not read from this field.
SecondScanIDWithResults	Int	The ScanID which actually has the results which were compared for the computer which was compared against the baseline computer. Do not read from this field.

LoggedOnUsers

The LoggedOnUsers table contains the list of logged on users on scanned machine.

Fields

Field Name	Type	Description
LoggedOnID	Int	PK
ScanID	Int	FK
UserType	Byte	Logged on user type. Possible values: 0 - Uninitialized. 1 - Locally logged on user. 2 - Remote logged on user.
UserName	nvarchar[255]	Windows user account name.
LogonDate	nvarchar[50]	Log on date and time in text format.
ElapsedTime	Int	The time that passed from LogonDate until now.
IdleTime	Int	Specifies the number of seconds the session has been idle. Only for remote logged on users. For locally logged on users the value is 0.
ItemsCount	Int	Specifies the number of files, devices, and pipes opened during the session for remote logged on users and program count taken from registry for locally logged on users.
UserFlags	Int	Describes how the user established the session. This member can be one of the following values. SESS_GUEST - The user specified by the sesi502_username member established the session using a guest account. SESS_NOENCRYPTION - The user specified by the sesi502_username member established the session without using password encryption.
ClientType	nvarchar[255]	For remote logged on users is a string that specifies the type of client that established the session. Some sample values are: “Windows 2002 Service Pack 2 2600”, “Windows 2000 2195”, “Windows Server 2003 3790”. For locally logged on users is the empty string “”.
Transport	nvarchar[255]	For remote logged on users is a string that specifies the name of the transport that the client is using to communicate with the server. Some sample values are: “\Device\NetbiosSmb”, “\Device\NetBT_Tcpip_{80853A48-D5DF-4D97-BEDF-EAFF6CA52B18}”. For locally logged on users is the empty string “”.
TTY	nvarchar[255]	The console used to log on the machine.
Application	nvarchar[255]	The application.
ComputerID	bigint	Not zero if part of Overview for that Computer.
LoggedOnUsersUid	nvarchar[36] uniqueidentifier	Unique row identifier.
Hash	nvarchar(40)	Content hash.

USBDevices

The USBDevices table contains USB devices that are plugged-in on the scanned machine.

Fields

Field Name	Type	Description
USBDevID	Int	PK
ScanID	Int	FK
Name	nvarchar[50]	Name of the connected USB device or name of the USB port detected.
Description	nvarchar[255]	Description of the connected USB device or description of the USB port detected.
Manufacturer	nvarchar[100]	USB device manufacturer.
ClassGuid	nvarchar[40]	Specifies the device-class GUID, formatted as shown here: **{***nnnnnnnn***-***nnnn***-***nnnn***-***nnnn***-***nnnnnnnnnnnn***}**, where each n is a hexadecimal digit. The device setup class GUID defines the

		..\CurrentControlSet\Control\Class\ClassGUID registry key under which to create a new subkey for any particular device of a standard setup class.
WhiteStatus	Int	This field tells if USB device is in LNSS configured whitelist or blacklist. Values: 0 – USB device is not in whitelist nor in blacklist 1 – USB device is whitelist 1 – USB device is in blacklist
Vendor	nvarchar[255]	The vendor of the detected USB device. (used for Linux)
SerialNumber	Nvarchar[255]	Serial number of device, e.g. “WD-WMA6S1451914”.
ComputerID	bigint	Not zero if part of Overview for that Computer.
USBDevicesUid	nvarchar[36] uniqueidentifier	Unique row identifier.
Hash	nvarchar(40)	Content hash.

WMINet

The WMINet table contains network devices detected using WMI on target machine.
The Hotfix table contains missing hotfixes of the installed products on scanned machine.

Fields

Field Name	Type	Description
WMINetID	Int	PK
ScanID	Int	FK
DeviceID	Int	Number that uniquely identifies a network device on the target machine.
CardName	nvarchar[255]	Name of the network card.
Description	nvarchar[255]	Network card description.
DHCPEnabled	nvarchar[20]	Boolean variable detailing if this interface is retrieving IP information via DHCP. Note: do not translate.
DHCPServer	nvarchar[50]	From which DHCP server the IP lease was obtained from.
Domain	nvarchar[255]	Represents the current domain on this network interface.
HostName	nvarchar[30]	The name of the host.
DeviceType	Int	Contains one of the following values: 1 – physical device 2 – virtual device 3 – software enumerated device 4 – wireless device 5 – unknown device type
MACAddress	nvarchar[18]	Device MAC address.
IPAddresses	nvarchar[255]	IP address of device.
DNSServers	nvarchar[255]	Nameserver of device.
Gateways	nvarchar[255]	Array of strings which would contain a list of IP addresses.
SSID	nvarchar[50]	Service set identifier. A unique identifier that stations must use to be able to communicate with an access point. The SSID can be any alphanumeric entry up to a maximum of 32 characters.
WEP	nvarchar[50]	The WEP (Wired Equivalent Privacy) text field describes the encryption level (if exists).
Status	nvarchar[20]	Text that describes the status of the network device. Examples: “Plugged in”, “Unplugged. Note: do not translate.
WhiteStatus	Int	This field tells if network card is in LNSS configured whitelist or blacklist. Values: 0 – network card is not in whitelist nor in blacklist 1 – network card is whitelist

		1 – network card is in blacklist
BCast	nvarchar[20]	The broadcast address. (used for Linux)
IP6	nvarchar[50]	The IPv6 address of the network card. (used for Linux)
Name	nvarchar[255]	The network card name. (used for Linux)
NMask	nvarchar[20]	The network mask. (used for Linux)
Vendor	nvarchar[255]	The network card's vendor. (used for Linux)
SerialNumber	Nvarchar[255]	Serial number of device, e.g. "WD-WMA6S1451914".
ComputerID	bigint	Not zero if part of Overview for that Computer.
WMINetUid	nvarchar[36] uniqueidentifier	Unique row identifier.
Hash	nvarchar(40)	Content hash.

MobileDevice

Contains other details about mobile devices.

Fields

Field Name	Type	Description
MobileDeviceID	Int	PK
ScanID	Int	FK
UniqueID	Nvarchar[255]	As unique as possible for each mobile device. We populate this field using an algorithm like: use PhoneNumber if available, if not, use IMEI if available etc.
MobileDeviceSourceID	Int	FK
PhoneNumber	Nvarchar[255]	E.g. 555157234.
Imei	Nvarchar [255]	International Mobile Station Equipment Identity (IMEI).
UserAgent	Nvarchar [255]	Sent to the web service which provides Exchange Active Sync or other services. E.g. Android/4.0.4-EAS-1.3.
FirstConnectTime	DateTime	Datetime of first sync.
LastConnectAttemptTime	DateTime	Datetime when sync was last tried.
LastSuccessConnectTime	DateTime	Datetime when sync was last performed successfully.
LastPolicyUpdateTime	DateTime	Datetime when the device policies were last synced.
Operator	Nvarchar[255]	Mobile operator. E.g. RO Vodafone RO.
MobileDevicePolicyID	Int	Id of the policy for this device.
ComputerID	bigint	Not zero if part of Overview for that Computer.
MobileDeviceUid	nvarchar[36] uniqueidentifier	Unique row identifier.
Hash	nvarchar(40)	Content hash.

Account

Contains details about a user. Currently, the user must be the owner of a mobile device or must use a mobile device.

Fields

Field Name	Type	Description
AccountID	Int	PK
AccountName	Nvarchar [255]	Account name. E.g. brunot.
DisplayName	Nvarchar [255]	E.g. Bruno Tinotti.
Domain	Nvarchar	E.g. test.org.

	[255]	
EmailAddress	Nvarchar [255]	brunot@test.org
UnmanagedMobileDevicesCount	Int	Number of unmanaged devices.
MobileDeviceSourceID	Int	FK
Department	Nvarchar [255]	Account department.
JobTitle	Nvarchar [255]	Account job title.

MobileDeviceToAccount

Contains a relationship between a mobile device and the users/owners/employees of the mobile device.

Fields

Field Name	Type	Description
MobileDeviceToAccountID	Int	PK
MobileDeviceID	Int	FK
AccountID	Int	FK

MobileDeviceSource

Contains details about mobile source.

Fields

Field Name	Type	Description
MobileDeviceSourceID	Int	PK
Type	Int	Possible values: 0 – unknown, 1 – Microsoft Exchange Server, 2 – Microsoft Office 365, 3 – Google Apps, 4 – Apple Profile Manager. Default 0.
Address	Nvarchar [255]	Represents the address server : IP or DNS.

MobileDevicePolicy

Contains information about exchange policies.

Fields

Field Name	Type	Description
MobileDevicePolicyID	Int	PK
Name	Nvarchar [255]	Name of the policy.
MobileDeviceSourceID	Int	Id of the source which contains this policy.

MobileDevicePolicyDetail

Contains details about exchange policies.

Fields

Field Name	Type	Description

MobileDevicePolicyDetailID	Int	PK
MobileDevicePolicyID	Int	Id of the policy.
Name	Nvarchar [255]	Name of the detail.
Value	Nvarchar [255]	Value of the detail.

AppInstalled

The AppInstalled table contains the applications installed on the scanned machine.

Fields

Field Name	Type	Description
AppInstalledID	Int	PK
AppName	nvarchar [255]	Name of the application.
SecurityAppType	Int	Type of security application. Values: 0 – normal application 1 – antivirus application 2 – antispyware application
IsRealtime	Int	Shows if security application works real time. Values: 0 – not detected 1 – not supported 2 – enabled 3 – disabled
IsUpToDate	Int	Shows if security application is updated. Values: 0 – not detected 1 – yes 2 – no 3 – not supported
LastUpdate	datetime	The date and time of the last update or NULL if not available.
Unauthorized	Int	Shows if security application is authorized. Values: 0 – Could not determine if app. is authorized or not. 1 – Application is unauthorized. 2 – Application is authorized.
AppVersion	nvarchar [255]	Specifies the version of the application.
AppPublisher	nvarchar [255]	The publisher (the company which made) of the application.
UninstallString	Memo	The string needed to uninstall the application without user interaction. The user should not be given the option to stop the application uninstall (i.e. no dialog with “Cancel” button, no cmd.exe window can be shown). If possible, no User Interface (UI) should be shown to the user.
ApprovedForSilentUninstal	Int	If the application can be uninstalled silently. Values: 0 – Unknown 1 – The application cannot be uninstalled silently. 2 – The application uninstalls itself completely silent and correct. The application was verified and approved by the user. 3 – The application can be uninstalled silently but was not approved by the user yet.
SerialNumber	nvarchar [255]	Product ID for application. E.g. “76588-652-7778751-50439”.
UserName	nvarchar [255]	Possible values: “” – all users. The application’s Add/Remove Programs entry is located in `HKEY_LOCAL_MACHINE\SOFTWARE\[Wow6432Node\]Microsoft\`

		`Windows\CurrentVersion\Uninstall` "<UserName>" – The application's Add/Remove Programs entry is located in `HKEY_USERS\<UserGUID>\SOFTWARE\[Wow6432Node\]Microsoft\Windows\CurrentVersion\Uninstall`, e.g. `HKEY_USERS\S-1-5-20\Software\Microsoft\Windows\CurrentVersion\Uninstall`
ProductKey	nvarchar [255]	Product key (also known as license key, CD key, serial etc.). E.g. "MNH2R-P8J2Y-6PKTK-VWJN6-Y868M".
Type	Number	Application type. Possible values: 0 – N/A, 1 – Operating system
Group	nvarchar [255]	Group name of application
InstallDate	DateTime	Install date of the software.

AppInstalledToScan

A table is needed in order to link the 3NF parent table with the Scan table.

Fields

Field Name	Type	Description
AppInstalledToScanID	Int	PK
ScanID	Int	FK
AppInstalledID	Int	FK
IsInCustomCategory	Int	
ComputerID	bigint	Not zero if part of Overview for that Computer.
Hash	nvarchar (40)	Content hash.

AppInstalledToScanToCategory

TABLE NAME:	AppInstalledToScanToCategory	
TABLE DESCRIPTION:	Used to link records from AppInstalled to the software category they belong to.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
AppInstalledToScanToCategoryID	AutoNumber (PK)	PK
AppInstalledToScanID	Number (FK)	FK
SoftwareCategoryID	Number (FK)	FK

SoftwareCategory

TABLE NAME:	SoftwareCategory	
TABLE DESCRIPTION:	Software categories specified by the user and default software categories.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
SoftwareCategoryID	AutoNumber (PK)	PK
Name	nvarchar[255]	Possible values: values defined by the user or OperatingSystem. Note: do not translate.
IsDefault	Number	Default 0. Possible values: 0 – not default, 1 – default.

Cache

The Cache table contains data which is cached between different moments of the scanning process on a machine or between scans on different machines. This way, some of the operations repeatedly executed during scan will be excuted only once and the common values will be stored in table **Cache**.
The information in this table is valid for an entire scanning, so this table is linked to **Scans** table with the foreign key *ScanID*.

Fields

Field Name	Type	Description
CacheID	Int	PK
ScansID	Int	FK
Name	nvarchar[255]	Name of the cached data. The name has to be unique on the scan.
Value	nvarchar[255]	The value of the cached data.

Processors

The Processors table contains all the processors of the scanned machine.

The machine for which the processors are retrieved is identified by the foreign key *ScanID*, which links the table with the primary key **ScanID** from table ***Scan***.

Fields

Field Name	Type	Description
ProcessorID	Int	PK
ScanID	Int	FK
Vendor	nvarchar[255]	The vendor of the processor.
Model	nvarchar[255]	Processor's model.
Speed	nvarchar[50]	The processor's speed.
Flags	nvarchar[255]	Specific processor flags.
Description	nvarchar[255]	E.g. EM64T Family 6 Model 15 Stepping 11.
ComputerID	bigint	Not zero if part of Overview for that Computer.
ProcessorsUid	nvarchar[36] uniqueidentifier	Unique row identifier.
Hash	nvarchar(40)	Content hash.

ComputerGroup

Each record from the *ComputerGroup* table has associated a group of computers as configured by the user.

TABLE NAME:	ComputerGroup	
TABLE DESCRIPTION:	Stores information about the groups defined by the user for the computers within his network.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
ComputerGroupID	AutoNumber (PK)	PK
Name	Text	Group name.
ParentGroupID	Number (FK)	The ID of the parent group. The value is NULL if it is a root group.
ComputerProfile	Text	The name of the assigned computer profile. If no computer profile is assigned to this computer group, the value stored in this field is the empty string ("").
IsInvisible	Number	Default 0. Possible values: 0 - Is visible, 1 - Is invisible.
ComputerGroupUid	nvarchar(36)	Unique computer group identifier across all installations of the product.

There is a special computer group named "LiveAgents" that is invisible.
There is a special computer group which contains all computers and computer groups that is invisible. A setting which is applied to this computer group is inherited by all computers and computer groups which do not have that setting already. See table GroupDetail for further information on this computer group.

GroupDetail

Each record from the *GroupDetail* table has associated a rule that defines a group of computers. The rule can be of one of the following types:

- include computers
- exclude computers

TABLE NAME:	GroupDetail	
TABLE DESCRIPTION:	Stores as scan targets the list of members of computer groups.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
GroupDetailID	AutoNumber (PK)	PK
ComputerGroupID	Number (FK)	The ID of the group for which we define the members details.
Type	Number	Can have the following values: 0 – Computer name 1 – Computer IP address 2 – Range of computers (including CIDR) 3 – Domain (or SMB workgroup) 4 – Active Directory Organizational Unit 6 - Text file 7 – All computers and computer groups 8 - Automatic attribute 9 - Attribute (non automatic) 10 – User Account (used by mobile devices)
Data	Text	The data which defines the group members according to the Type field.
Exception	Number	Can have the following values: 0 – Default value 1 – If this rule is an exception rule

There are special types of records for this table with the properties shown below.

Type	Data	Observations
3	Primary domain	
7	AllComputersAndComputerGroups	A hidden computer group which contains all computers and all computer groups. In order to get the correctly translated name for this field, read the field Name from the table ComputerGroup.

Computer

TABLE NAME:	Computer	
TABLE DESCRIPTION:	Used to uniquely identify a computer.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
ComputerID	AutoNumber (PK)	PK
Name	Text	Computer name. If this computer is a mobile device (Type=2) the field Name has value <EmailAddressOfAccount> (<MobileDeviceHardwareModel>) e.g. “rumbj@test.com (Google Nexus 4)”.
DnsName	nvarchar[255]	DNS fully qualified computer name.
IP	Text	Computer IP
MAC	Text	Computer MAC address

DistinguishedName	Text	The Distinguished Name (DN) of the computer as an object in Active Directory/Directory Services. Uniquely identifies a computer. E.g. "CN=V2003STA64,CN=Computers,DC=accounting,DC=dom".
IsLicensed	Number	Can have the following values: 0 – N/A, 1 – The user selected the computer as being licensed, 2 - The user selected the computer as being not licensed
Timestamp	Date/Time	Date when the computer identification information was up to date.
Type	Number	Default 0. Possible values: 0 - Workstation, 1 - Server, 2 – Mobile device.
Domain	nvarchar[255]	Domain that the machine is joined to.
UniqueID	nvarchar[255]	Computer unique identifier
ComputerUid	nvarchar(36)	Unique computer identifier across all installations of the product.

ComputerLatestData

TABLE NAME:	ComputerLatestData	
TABLE DESCRIPTION:	Acts as a backing store for reporting and other UI modules. Frequently displayed up to date information about computers.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
ComputerLatestDataID	AutoNumber (PK)	PK
ComputerID	Number (FK)	FK to field ComputerID from the table Computer.
OverviewVulnerabilityLevel	Int	The current complete overview level for the computer.
AuthenticationIssuesWereEncountered	Int	Value = “1” when any authentication issues are encountered.
ScanFailedBecauseComputerIsNotLicensed	Int	Possible values: 0 – N/A, 1 – computer is not licensed, 2 – computer is licensed.
OperatingSystem	Text	See Scan.OS. E.g. "Windows XP x64".
ServicePack	Text	See Scan.ServPack. E.g. "2".
NetworkRole	Text	See Scan.Usage. E.g. “Workstation”.
LanguageID	Text	See Scan.Language. E.g. "0409".
IsVirtualMachine	Int	Possible values: 1 - the scanned machine is a virtual machine.
VirtualizationTechnology	Text	See Scan.VirtualizationTechnology. E.g. “”.
LastScanned	DateTime	
AgentStatus	Int	Possible values: 0 - Agent not installed or not managed by us, 1 - Pending agent install, 2 - Pending agent uninstall, 3 - Agent is installed.
MissingPatchesSensor	Int	Possible values: 0 – Disabled, 1 – Green, 2 – Red
MissingServicePacksSensor	Int	Possible values: 0 – Disabled, 1 – Green, 2 - Red
VulnerabilitiesSensor	Int	Possible values: 0 – Disabled, 1 – Green, 2 - Red
MalwareProtectionSensor	Int	Possible values: 0 – Disabled, 1 – Green, 2 - Red
FirewallSensor	Int	Possible values: 0 – Disabled, 1 – Green, 2 - Red
UnauthorizedApplicationsSensor	Int	Possible values: 0 – Disabled, 1 – Green, 2 - Red
AuditingSensor	Int	Possible values: 0 – Disabled, 1 – Green, 2 - Red

CredentialsSensor	Int	Possible values: 0 – Disabled, 1 – Green, 2 – Red
AgentHealthSensor	Int	Possible values: 0 – Disabled, 1 – Green, 2 – Red
Domain	Text	See Scan.Domain. E.g. "DOM".
OrganizationalUnit	Text	See Scan. OrganizationalUnit. E.g. "OU=OU_COMPUTERS,DC=DOM".
LastAudited	DateTime	The last time when a security scan with a significant profile was last performed.
RelayStatus	Int	Default 0. Possible values: 0 - Inactive, 1 - Pending activation, 2 - Active, 3 - Pending deactivation
Hardware	nvarchar[255]	The name of the hardware of the machine. E.g. Google Nexus 4.
RebootRequired	Number	0 – reboot is not required 1 – reboot is required
SSHPort	Number	Default = 0
AccountEmailAddress	nvarchar[255]	See field EmailAddress from table Account.
LastSuccessConnectTime	DateTime	See field LastSuccessConnectTime from table MobileDevice.
PhoneNumber	nvarchar[255]	See field PhoneNumber from table MobileDevice.
Manufacturer	nvarchar[255]	See field ComputerSystem.Manufacturer
ModelName	nvarchar[255]	See field ComputerSystem.ModelName
OSInstallDate	DateTime	See field ComputerSystem.OSInstallDate
FormFactor	Number	See field ComputerSystem.FormFactor
Department	nvarchar[255]	See field Account.Department
DisplayName	nvarchar[255]	See field Account.DisplayName
JobTitle	nvarchar[255]	See field Account.JobTitle
ServiceTag	nvarchar[255]	See field ComputerSystem.ServiceTag

ComputerAgregateData

TABLE NAME:	ComputerAgregateData	
TABLE DESCRIPTION:	Last data for computer from overview panel Results Statistics.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
ComputerAgregateDataID	AutoNumber (PK)	PK
ComputerID	Number (FK)	ID of the computer.
MissingSecurityUpdatesCount	Int	Number of Missing Security Updates.
MissingCriticalSecurityUpdatesCount	Int	Number of Missing Critical Security Updates.
MissingNonSecurityUpdatesCount	Int	Number of Missing Non Security Updates.
MissingServicePacksCount	Int	Number of Missing Service Packs.
OtherVulnerabilitiesCount	Int	Number of Other Vulnerabilities.
OtherCriticalVulnerabilitiesCount	Int	Number of Other Critical Vulnerabilities.
PotentialVulnerabilitiesCount	Int	Number of Potential Vulnerabilities.
InstalledApplicationsCount	Int	Number of Installed Applications.
OpenPortsCount	Int	Number of Opened Ports.
SharesCount	Int	Number of Shares.
USBDevicesCount	Int	Number of USB Devices.
ServicesCount	Int	Number of Services.
NetworkDevicesCount	Int	Number of Network Devices.
ProcessesCount	Int	Number of Processes.

LoggedOnUsersCount	Int	Number of Logged On Users.
InstalledServicesPacksCount	Int	Number of Installed Services Packs.
InstalledSecurityUpdatesCount	Int	Number of Installed Security Updates.
InstalledNonSecurityUpdatesCount	Int	Number of Installed Non Security Updates.
MajorVersionUpgradesCount	Int	Number of Major Version Upgrades.

ComputerIndicator

TABLE NAME:	ComputerIndicator	
TABLE DESCRIPTION:	Information which belongs to a computer but is not necessarily the result of a scan (could be the result of a deployment of agent management etc.).	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
ComputerIndicatorID	AutoNumber (PK)	PK
ComputerID	Number (FK)	FK to field ComputerID from the table Computer.
Iid	Text	The installation ID of the product.
Name	Text	Unique name of the detail.
Value	Text	Value of the detail.

Possible values for the field Name:

Name	Observations
AuthenticationIssuesWereEncountered	Value = “1” when any authentication issues are encountered.
OperatingSystem	See Scan.OS. E.g. "Windows XP x64".
ServicePack	See Scan.ServPack. E.g. "2".
NetworkRole	See Scan.Usage. E.g. “Workstation”.
VirtualizationTechnology	See Scan.VirtualizationTechnology. E.g. “”.
LanguageID	See Scan.Language. E.g. "0409".
IsVirtualMachine	Possible values: 1 - the scanned machine is a virtual machine.

HostnameToIid

TABLE NAME:	HostnameToIid	
TABLE DESCRIPTION:	Contains a list of all the product installations which have used this database as the scan results database.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
HostnameToIidID	AutoNumber (PK)	PK
Hostname	Text	E.g. "SRVX64".
Iid	Text	The installation ID of the product.
Timestamp	Date/Time	Date when the record was last modified.

ComputerSetting

TABLE NAME:	ComputerSetting	
TABLE DESCRIPTION:	Contains settings that are made per computer or per computer group. E.g. credentials to use when scanning a computer.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
ComputerSettingID	AutoNumber (PK)	PK
ComputerID	Number	The ID of the computer that uses this setting.
ComputerGroupID	Number	The ID of the computer group that uses this setting.

CategoryName	Text	The category of settings to which this setting belongs.
ItemName	Text	The name of the setting.
ItemValue	Text	The value of the setting.
ComputerSettingIDFromParent	Number	If > 0, then this setting is identical to the one from the parent computer group with ComputerSettingID (the setting is inherited from a parent computer group).
Timestamp	Date/Time	Date when the setting was last modified.

Some of the possible categories and items from this table are shown below.

CategoryName	ItemName	Observations
AutoRemediationOptions	WarnUser	Do not implement StopServices, ServicesList.
	CustomShare	
	RebootAndShutdown	
	DeleteFiles	
	ThreadCount	
	Timeout	
	Guid3	
	Guid4	
	Guid1	
	Guid2	
	DeployWithOriginalNames	
	AutodeployPatches	
	AutodeployServicePacks	
	AutouninstallApplications	
Logon	Type	
	Username	
	Data1	Contains the encrypted password.
Agent	UseResidentAgent	Possible values: • Null – not set, inherited from parent group • 0 – do not use resident agents • 1 – use resident agents
	ScanRecurrence	FK to Recurrence table.
	IsScanRecurrenceEnabled	Possible values: 0 – the user does not want this type of recurrence at all, 1 – enabled, you can use the value of the item ScanRecurrence
	ScanNow	Default 0. If value is 1, the agent management system will trigger a new scan.
ComputerGroup	RefreshGroupMembersListRecurrence	FK to Recurrence table.
	IsRefreshGroupMembersListRecurrenceEnabled	Possible values: 0 – the user does not want this type of recurrence at all, 1 – enabled, you can use the value of the item RefreshGroupMembersListRecurrence
	IsRefreshGroupMembersListTargetARecursiveOU	Do not use this value if the computer group (which has the settings) is not an OU. Possible values: 0 – do not scan the OU recursively, 1 – scan the OU recursively.
Ignore_MissingPatch	The text from field Title from the table Patches.	Is ScanProfileOverride.
Acknowledge_MissingPatch	The text from field Title from the table Patches.	Is ScanProfileOverride.

Ignore_Backdoor	The text from field Value from the table Backdoors.	Is ScanProfileOverride.
Ignore_Vulnerability	The text from field Name from the table Alert.	Is ScanProfileOverride.
Acknowledge_Vulnerability	The text from field Name from the table Alert.	Is ScanProfileOverride.
ChangeSeverity_Vulnerability	The text from field Name from the table Alert.	Is ScanProfileOverride.
Reset_ThreatLog	One text which says that viruses were found, another text which says that spyware was found.	Is ScanProfileOverride.

Recurrence

TABLE NAME:	Recurrence	
TABLE DESCRIPTION:	Contains a recurrence like “Occurs every Monday, Wednesday, Saturday and Sunday at 3:00:00 PM.”.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
RecurrenceID	AutoNumber (PK)	PK
Type	Number	Possible values: -1 – run once at specified time, 0 – daily recurrence,1- weekday, 2 – weekly ,3- monthly exact day, 4 - monthly ordinal day
Date	Text	The date and time when the last recurrence occurred. Used for all values from field Type. Format: <Year4Digits><Month2Digits><Day2Digits><Hour2Digits><Minutes2Digits><Seconds2Digits> yyyyMMddHHmmss(.NET), %Y%m%d%H%M%S(C++), yyyymmddhhnnss(Delphi). E.g.: “20110221150553” (means: ”The last occurrence took place on 21st of February 2011 at 15:05:53”).
Time	Text	The time of the recurrence. Used for: Type >= 0. Format: <Hour2Digits>:<Minutes2Digits>:<Seconds2Digits>. HH:mm:ss(.NET), %H:%M:%S(C++), hh:nn:ss(Delphi). E.g.: “150000” (means: ”This recurrence should occur at 15:00:00”).
DailyPeriod	Number	The recurrence period in days. Used for: Type = 0. E.g.: 10 (means: ”Occurs every 10 days at Time ”).
WeeklyPeriod	Number	The recurrence period in weeks. Used for: Type = 2. E.g.: 3 (means: ”Occurs every 3 weeks on WeeklyDays at Time. ”).
WeeklyDays	Text	The days of the week in which the weekly recurrence occurs. Used for: Type = 2. Format: A text with length of exactly 7 characters containing only ‘0’ and ‘1’, where ‘1’ means that recurrence will occur in that specific day of the week and ‘0’ means it will not. The first day of the week is Sunday. E.g.: “1001000” (means: ”Occurs every WeeklyPeriod weeks on Sunday and Wednesday at Time. ”).
MonthlyExactDayDay	Number	The day of the month when the monthly exact day recurrence occurs. Used for: Type = 3. E.g.: 2 (means: ”Occurs on day 2 of every MonthlyExactDayPeriod months at Time. ”).
MonthlyExactDayPeriod	Number	The recurrence period in months for monthly exact day recurrence. Used for: Type = 3. E.g.: 6 (means: ”Occurs on day MonthlyExactDayDay of every 6 months at Time. ”).
MonthlyOrdinalDayOrdinal	Number	Ordinal index for monthly ordinal day. Used for: Type = 4. Possible values: 0 – First, 1 – Second, 2 – Third, 3 – Fourth, 4 – Last.

		E.g.: 4 (means: ”Occurs on the last MonthlyOrdinalDayDayName of every MonthlyOrdinalDayPeriod months at Time. ”).
MonthlyOrdinalDayDayName	Number	Ordinal specifier for monthly ordinal day. Used for: Type = 4. Possible values: 0 – Day, 1 – Weekday, 2 – Weekend Day, 3 – Sunday, … 9 – Saturday. E.g.: 1 (means: ”Occurs on MonthlyOrdinalDayOrdinal Weekday of every MonthlyOrdinalDayPeriod months at Time. ”).
MonthlyOrdinalDayPeriod	Number	The recurrence period in months for monthly ordinal day recurrence. Used for: Type = 4. E.g.: 3 (means: ”Occurs on MonthlyOrdinalDayOrdinal MonthlyOrdinalDayDayName of every 3 months at Time. ”).
RunOnceDateTime	Text	The date and time when the Run Once is ought to occur. Used for: Type = -1. Format: <Year4Digits><Month2Digits><Day2Digits><Hour2Digits><Minutes2Digits><Seconds2Digits> yyyyMMddHHmmss(.NET), %Y%m%d%H%M%S(C++), yyyymmddhhnnss(Delphi). E.g.: “20110221150553” (means: ”This ‘Run Once recurrence’ ought to occur on 21st of February 2011 at 15:05:53”).
ForcedOccurNow	Number	By setting this flag on 1 an occurrence will be forcefully triggered without affecting the recurrence schedule (unless the recurrence is Type = -1 [aka Run Once]). Used for: All Type values. E.g.: 1 (means: ”Force an occurrence ASAP.”).
ForcedLastDateTime	Text	The date and time when the last forced occurrence was triggered. Used for: All Type values. Format: <Year4Digits><Month2Digits><Day2Digits><Hour2Digits><Minutes2Digits><Seconds2Digits> yyyyMMddHHmmss(.NET), %Y%m%d%H%M%S(C++), yyyymmddhhnnss(Delphi). E.g.: “20110221150553” (means: ”The last forced occurrence was triggered on 21st of February 2011 at 15:05:53”).

Wherever possible, in our product, the default values for recurrence are:

Recurrence Field	Default Value
Type	0
Date	""
Time	15:00:00
DailyPeriod	1
WeeklyPeriod	1
WeeklyDays	1111111
MonthlyExactDayDay	1
MonthlyExactDayPeriod	1
MonthlyOrdinalDayOrdinal	0
MonthlyOrdinalDayDayName	0
MonthlyOrdinalDayPeriod	1
RunOnceDateTime	""
ForcedOccurNow	0
ForcedLastDateTime	""

ScanProfileOverride

TABLE NAME:	ScanProfileOverride	
TABLE DESCRIPTION:	Stores changes which are being made by the user to all scanning profiles on a per computer basis. E.g. missing patches which should be ignored.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
ScanProfileOverrideID	AutoNumber (PK)	PK
ComputerSettingID	Number	FK to table ComputerSetting.
StartTimestamp	Date	The date and time since when this rule applies.
EndTimestamp	Date	The date and time until when this rule applies.
OriginalAlertLevel	Number	The original value from the scanning profiles. See field Level from table Alert.
NewAlertLevel	Number	Consider this value instead of the value from field Level from table Alert. See field Level from table Alert.
DisplayName	Text	Text to show in viewer. Currently the values are from PatchesLocalizedData.Title, Alert.Name, Backdoors.Value.
Reason	Memo	Reason provided by the administrator for the ignore/acknowledge/change.
I1	Number	Reserved for future use.
I2	Number	Reserved for future use.
S1	Text	Reserved for future use.
S2	Text	Reserved for future use.
S3	Text	Reserved for future use.
M1	Memo	Reserved for future use.

ComputerToGroup

TABLE NAME:	ComputerToGroup	
TABLE DESCRIPTION:	Used to link computers from the database to the groups they belong to.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
ComputerToGroupID	AutoNumber (PK)	PK
ComputerID	Number (FK)	The ID of the computer.
ComputerGroupID	Number (FK)	The ID of the group of the computer.

CategoryOfResults

TABLE NAME:	CategoryOfResults	
TABLE DESCRIPTION:	For a given record in the Scan table, stores the information about the categories of security scan results available.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
CategoryOfResultsID	AutoNumber (PK)	PK
ScanID	Number (FK)	FK to field ScanID from the table Scan.
ResultsCategoryName	NVarchar[255]	Unique name of the category of information from the security scanner results.
WasCollected	Number	Default 0. 0 – if the category of results was not collected (possible causes: could not connect to computer, scanning for this category of scan results is disabled from the scan profile etc.). 1 - if the category of results was collected (possible causes: success, all of the information that can be collected is disable/blacklisted from the scan profile etc.).
ResultsDidNotChangeSinceScanID	Number	Default 0. Different from 0 if the scan results belong to a scheduled agent and the category of scan results did not change (in this case, this field contains the ScanID that contains the exact same information as the one collected during this scan).

MessageName	NVarchar[255]	Unique name of the message. Is not translated.

What is the List of Categories of Scan Results Information?

The categories of scan results information define the granularity with which:

- the scan results DB is updated after scan results from agents are available. See the mechanism for avoiding results duplication for agent scans.

Some of the possible values for the field ResultsCategoryName from this table are shown below.

CategoryName	Observations
Vulnerabilities	
MissingServicePacks	
MissingPatches	
InstalledServicePacks	
InstalledPatches	
TcpPorts	
UdpPorts	
ComputerInformation	Computer Information (SMB, server, PDC, BDC)
Shares	
Users	
UserGroups	
Domains	
LoggedOnUsers	
Drives	
TimeOfDay	
Registry	
Services	
Sessions	
PasswordPolicies	
Processes	
SecurityAuditPolicies	
VirtualizationTechnology	
HardwareDevices	
Software	

OverviewCategory

TABLE NAME:	OverviewCategory	
TABLE DESCRIPTION:	For a given computer at a given place in time, stores the complete picture of security scan results available.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
OverviewCategoryID	AutoNumber (PK)	PK
ComputerID	Number (FK)	FK to field ComputerID from the table Computer.
ResultsCategoryName	NVarchar[255]	Unique name of the category of information from the security scanner results.
ScanIDOfActualResults	Number	The ID of the record from the Scan table that contains the information for this results category. Default 0. Points to field ScanID from the table Scan. Not all records from this table have this field <> 0. Equal to the value in field ScanIDOfLastScanThatCouldCollectInformation for all scan results except for those belonging to scheduled agents.
ScanIDOfLastScanThatCouldCollectInformation	Number	The ID of the record from the Scan table that contains the latest scan that collected the information for this

		results category. Default 0. Points to field ScanID from the table Scan. Not all records from this table have this field <> 0. Equal to the value in field ScanIDOfActualResults for all scan results except for those belonging to scheduled agents.
MessageName	NVarchar[255]	Unique name of the message. Is not translated.
LastCollected	Date/Time	Timestamp of last scan that collected information for this category.

OverviewComparison

TABLE NAME:	OverviewComparison	
TABLE DESCRIPTION:	For a given computer at a given place in time, stores the list of changes since the previous place in time.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
OverviewComparisonID	AutoNumber (PK)	PK
ScanID	Number	The ScanID which represents the overview for which to generate history for this computer. Do not read this field.
PreviousScanID	Number	The ScanID which represents the immediately previous overview for the same computer. Do not read this field.
DeploymentsID	Number	Can be 0. See field DeploymentsID from the table Deployments.
ComputerID	Number	Can be 0. See field ComputerID from the table Computer.
Timestamp	Date/Time	The date and time when this change occurred.
ResultsCategoryName	NVarchar[255]	The category of information. E.g. "HardwareDevices".
Type	Number	Detailed category of information. E.g. 38 (DisplayAdapters). See field CompareType from table Compare.
Title	NVarchar[255]	Short description of the change. E.g. "Removed display adapter".
Text	Ntext	Complete information about this change since the previous place in time. E.g. "Device 'Samsung SyncMaster 12-4581' has been removed."
ScanIDWithResults	Int	The ScanID which represents the ScanID which actually has the results which were compared. Do not read from this field.
PreviousScanIDWithResults	Int	The ScanID which represents the previous ScanID for the same computer which actually has the results which were compared. Do not read from this field.
DeploymentID	Int	Can be 0. See field DeploymentID from the table Deployment. Do not read from this field.

Indicator

TABLE NAME:	Indicator	
TABLE DESCRIPTION:	For a given entry in the Scan table, stores information that needs to be accessed quickly. E.g. the overview vulnerability level.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
IndicatorID	AutoNumber (PK)	PK
ScanID	Number (FK)	FK to field ScanID from the table Scan.
Name	NVarchar[255]	Unique name of the detail.
Value	NVarchar[255]	Value of the detail.
ComputerUid	nvarchar[36]	Unique identifier of the Computer.

Possible values for the field Name:

Name	Observations
OverviewVulnerabilityLevel	

ScansError

Various errors can occur in the course of a security scan that have nothing to do with a particular computer, e.g. network discovery errors, licensing errors, WinSock errors, security scanner initialization errors etc.

Fields

Field Name	Type	Description
ScansErrorID	Int	PK
ScansID	Int	FK
Text	nvarchar[255]	Error text.
WindowsErrCode	nvarchar[255]	Windows error code. Note: do not translate.
Context	nvarchar[255]	Not used yet.
Timestamp	Date/Time	The date and time when the error occurred.

Agent

TABLE NAME:	Agent	
TABLE DESCRIPTION:	The latest details about a security scanner agent.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
AgentID	AutoNumber (PK)	PK
ComputerID	Number (FK)	ID of the computer where the security scanner agent runs.
Status	Number	Default 0. 0 - agent is not installed, 1 - agent is installed.
TimestampOfLastResultsImport	Date	Date when the last scan results import was made.
TimestampOfLastProfilesUpdate	Date	Last known operationsprofiles.mdb modification date on the agent.
AgentManagerErrorCode	NVarchar[255]	Default 0. Possible values: 0 – Success, 1 – Computer not online, 2 – Access denied, 3 – Failed to install the agent, 4 – Failed to upgrade the agent, 5 – Computer not licensed, 6 – Other error
AgentManagerErrorText	NVarchar[255]	Text describing errors encountered during agent management operation. This text is in the language of the user interface. E.g. "The RPC server is not available.".
TimestampOfLastRecurrenceUpdate	Date	Date of the last update to the recurrence setting of the agent.
BuildNumber	NVarchar[255]	Build number of the agent installation.
ScanStatus	Number	Possible values: 0 - no scan in progress, 1 - scan in progress.
TimestampOfLastScanStatusNotification	Date/Time	Timestamp when the last scan start notification was received.
ScanProfile	NVarchar[255]	Name of scanning profile that the agent should use.
TimestampOfLastAgentDeploymentAttempt	Date	Timestamp of the last agent deployment operation attempt.
TimestampOfSuccesfulAgentDeployment	Date	Date when the agent was deployed.
TimestampOfLastSuccessfulAgentAction	Date	Date when we last found the computer online and confirmed the good health of the agent.
AgentScanRecurrenceDisplayName	NVarchar[255]	A recurrence converted to a human readable format. E.g. Scan run daily at 12:00 PM.
RelayToUse	Number	Default 0: The ComputerID of the computer that is to be used by an agent as relay when performing tasks for this Main installation.
TimestampOfLastRelayClie	Date	The moment when an agent last received the settings

ntConfigurationUpdate		as relay client (relay to use).
WorkingHours	NVarchar[255]	Specifies the hours in which an agent can update patches definitions.
AgentUID	NVarchar[255]	Unique ID for a better identification of Agent.

AgentUpdateJobs

TABLE NAME:	AgentUpdateJobs	
TABLE DESCRIPTION:	Update jobs that have executed on agents.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
AgentUpdateJobID	AutoNumber (PK)	PK
AgentID	Number (FK)	ID of the agent where the update job was done.
Status	Number	Default 0. 1 - success, 2 – partial, 3 – failed, 4 – cancelled, 5 - postponed.
EndTime	Date	Date when the job was complete.
StartDate	Date	Date when the job was started.

AgentUpdateJobPackages

TABLE NAME:	AgentUpdateJobPackages	
TABLE DESCRIPTION:	Update packages and their status for update jobs that executed on agents.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
AgentUpdateJobPackageID	AutoNumber (PK)	PK
AgentUpdateJobID	Number (FK)	ID of the agent update job which included this package.
Status	Number	Default 0. 1 - success, 2 – failed, 3 – cancelled, 4 - postponed.
DownloadedFileName	NText	The name of the downloaded file.
LongName	NText	Package long/display name.
Name	NVarchar[255]	Package short name (This also acts as a package identifier).
PublishDate	Date	Date when package was published.
Size	Number	Default 0. File size in bytes.
Version	Number	Default 0. Package version.

Relay

TABLE NAME:	Relay	
TABLE DESCRIPTION:	The latest details about a relay.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
RelayID	AutoNumber (PK)	PK
ComputerID	Number (FK)	ID of the computer where the relay runs.
Status	Number	Default 0. 0 - relay is inactive, 1 - relay active.
CacheDirectory	NVarchar[255]	E.g. "c:\ProgramData\GFI\LanGuard 10\RelayCache\".
PortWhereToServe	Number	E.g. 1070.
TimestampOfLastConfigurationUpdate	Date	The moment when a computer last received the relay settings (role, port, caching folder).
RelayManagerErrorCode	Number	Default 0: Error codes to be decided.
RelayManagerErrorText	NVarchar[255]	Error message resulted while managing a relay.

ComputerGroupEffectiveMember

TABLE NAME:	ComputerGroupEffectiveMember
TABLE DESCRIPTION:	For a given computer group contains the list of all computers found in this computer group or recursively in any computer group contained in this

	computer group.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
ComputerGroupEffectiveMemberID	AutoNumber (PK)	PK
ComputerGroupID	Number (FK)	ID of the computer group.
ComputerID	Number (FK)	ID of the computer.

CurrentSelection

TABLE NAME:	CurrentSelection	
TABLE DESCRIPTION:	Contains the list of computers which are currently selected in the user interface part of a given installation of the product.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
CurrentSelectionID	AutoNumber (PK)	PK
ComputerID	Number	ID of the computer.
IsSelected	Number	Possible values: 0 - currently not selected, 1 - currently selected.
IsFilteredOut	Number	Possible values: 0 - is not filtered out, 1 - is filtered out.
ApplicationUserSessionID	Number	ID of the session.

Selection

TABLE NAME:	Selection	
TABLE DESCRIPTION:	Contains a list of computers. Needed for scheduled reports.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
SelectionID	AutoNumber (PK)	PK
ComputerID	Number	ID of the computer.
IsSelected	Number	Possible values: 1 - currently selected.
SessionID	NVarchar[255]	Unique ID (e.g. GUID) of this session of selection of computers.
TimestampOfSession	DateTime	Timestamp associated to this session of selection of computers.

Software

TABLE NAME:	Software	
TABLE DESCRIPTION:	Contains all of the software products detected by OESIS Local. Contains the types of information that are common to all software product types.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
SoftwareID	AutoNumber (PK)	PK
ScanID	Number (FK)	FK to field ScanID from the table Scan.
ProductID	Number	Unique identifier for a software product supported by OESIS Local.
Version	NVarchar[255]	
VendorName	NVarchar[255]	
Name	NVarchar[255]	
ExpirationDate	DateTime	
InstallDir	NVarchar[255]	
LicenseType	Number	Possible values: -1 – N/A, 1 – trial, 2 – monthly subscription, 3 – annual, 4 - perpetual (never expires), 5 - product is not licensed currently
GuiLanguageID	Number	Language ID of the software product's Graphical User Interface.
UpdateUri	Ntext	The location of the update server for this product. E.g. "http://windowsupdate.microsoft.com, https://windowsupdate.microsoft.com".
IsExpired	Number	Possible values: -1 – N/A, 0 – is not expired, 1 – is

		expired
IsAuthentic	Number	Possible values: -1 – N/A, 0 – signed and trusted, 1 - not signed, 2 – invalid signature, 3 – not trusted, 4 – access denied, 5 - unknown
Capabilities	Ntext	Lists all of the interfaces and methods that OESIS Local supports for this product. The values are space separated, e.g. “IAntivirus::SetRTP IAntivirus::Scan”.
ComputerUid	nvarchar[36]	Unique identifier of the Computer.

Some of the important capabilities are shown below.

Capability	Observations
ISoftwareProduct::UpdateProduct	
ISoftwareProduct::UninstallProduct	
IAntivirus::SetRTP	
IAntivirus::Scan	
IAntivirus::Antivirus_FullSystemScan	
IAntispyware::SetAntispyFileSystemProtectionStatus	
IAntispyware::AntispyScan	
IAntispyware::Antispyware_FullSystemScan	
IFirewall::EnableFirewall	
IFirewall::DisableFirewall	
IFirewall::AllowPort	
IFirewall::BlockPort	
IFirewall::AllowApp	
IFirewall::BlockApp	
IVirtualMachine::StartVM	
IVirtualMachine::PauseVM	
IVirtualMachine::StopVM	
IVirtualMachine::ResumeVM	

SoftwareDetail

TABLE NAME:	SoftwareDetail	
TABLE DESCRIPTION:	Contains additional information about software products.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
SoftwareDetailID	AutoNumber (PK)	PK
SoftwareID	Number (FK)	FK to field SoftwareID from the table Software.
Category	NVarchar[255]	Category of detail.
Name	NVarchar[255]	Unique name of the detail.
Value	Ntext	Value of the detail.

Some of the possible categories and items from this table are shown below.

Category	Name	Value	Observations
SoftwareProduct	ServiceInfo	Contains details about a service installed by the software product. E.g. “AVP (Windows 2000, 24419db0ad42b68caffa6bf903be364a)”.	
DiskEncryptionSoftware	SupportedEncryptionAlgorithm	Contains details about one of the encryption algorithms supported by the disk encryption software. E.g. “Serpent Twofish AES (128, XTS)”.	See table DiskEncryptionLocations for details.
BackupSoftware	ScheduleInfo	E.g. “1 600”. The second integer represents the number of seconds (or worst case number of seconds) between 2 backup operations. It is only returned in	

		the relevant cases. The first integer has the following possible values: 0 – not currently scheduled, 1 – unknown, 2 - the backup services are running, but it is uncertain if there is a scheduled backup specified, 3 - a backup is currently scheduled, we're returning the worst case time, 4 - a backup is currently scheduled, we're returning accurate time, 5 - the product supports automatic backups and it is enabled (when files been changed), 6 - performing backup when idle (usually when CPU is really low).	

SoftwareUpdate

TABLE NAME:	SoftwareUpdate	
TABLE DESCRIPTION:	Contains information about the updates of software products.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
SoftwareUpdateID	AutoNumber (PK)	PK
SoftwareID	Number (FK)	FK to field SoftwareID from the table Software.
IsUpdateLatest	Number	If the installed software has the latest updates. Posible values: 0 - N/A, 1 - is update latest, 2 - is not update latest
IsEngineLatest	Number	If the installed software has the latest engine. Posible values: 0 - N/A, 1 - is engine latest, 2 - is not engine latest
DefinitionTime	DateTime	For the latest updates available on the installed product's update site: the release date/time for the definitions.
DefinitionVersion	NVarchar[255]	For the latest updates available on the installed product's update site: the release version for the definitions. E.g. “7.10.07.163”.
DefinitionSignature	NVarchar[255]	For the latest updates available on the installed product's update site: additional information about the release version for the definitions. E.g. “75926”.
EngineVersion	NVarchar[255]	For the latest updates available on the installed product's update site: the version of the engine. E.g. “7.31824”.
ProductType	Number	Possible values: 1 – antivirus, 2 – antispyware, 4 – personal firewall, 8 – application firewall.

AntiPhishingSoftware

TABLE NAME:	AntiPhishingSoftware	
TABLE DESCRIPTION:	Additional information which is specific to this type of software products. Collected by OESIS Local.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
AntiPhishingSoftwareID	AutoNumber (PK)	PK
SoftwareID	Number (FK)	FK to field SoftwareID from the table Software.
EnabledForApplications	NVarchar[255]	The values are comma separated, e.g. “Internet Explorer, Google Chrome, Opera”.
InstalledForApplications	NVarchar[255]	The values are comma separated, e.g. “Internet

		Explorer, Google Chrome, Opera".
SupportedApplications	NVarchar[255]	The values are comma separated, e.g. "Internet Explorer, Google Chrome, Opera".

WebBrowserSoftware

TABLE NAME:	WebBrowserSoftware	
TABLE DESCRIPTION:	Additional information which is specific to this type of software products. Collected by OESIS Local.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
WebBrowserSoftwareID	AutoNumber (PK)	PK
SoftwareID	Number (FK)	FK to field SoftwareID from the table Software.
ProxyMode	Number	Possible values: -1- N/A, 1 – manual proxy, 2 – automatic proxy, 3 – no proxy, 4 – auto detect proxy. ? //TODO: Ask OPSWAT
ProxyIP	NVarchar[255]	
ProxyPort	NVarchar[255]	
IsCertCompliant	Number	-1 – N/A, 0 – not CERT compliant, 1 - if the security settings of the browser are compliant with the standard defined by the CERT Program (http://www.cert.org/tech_tips/securing_browser/).
IsDefaultBrowser	Number	-1 – N/A, 0 – not the default web browser, 1 – the default web browser.
PopUpBlocker_IsEnabled	Number	-1 – N/A, 0 – disabled, 1 – enabled

HealthAgentSoftware

TABLE NAME:	HealthAgentSoftware	
TABLE DESCRIPTION:	Additional information which is specific to this type of software products. Collected by OESIS Local.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
HealthAgentSoftwareID	AutoNumber (PK)	PK
SoftwareID	Number (FK)	FK to field SoftwareID from the table Software.
IsAgentRunning	Number	-1 – N/A, 1 – is running, 0 – is not running
IsSystemInCompliance	Number	If the system is in compliance with the policy. -1 – N/A, 1 – true, 0 – false

DiskEncryptionSoftware

TABLE NAME:	DiskEncryptionSoftware	
TABLE DESCRIPTION:	Additional information which is specific to this type of software products. Collected by OESIS Local.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
DiskEncryptionSoftwareID	AutoNumber (PK)	PK
SoftwareID	Number (FK)	FK to field SoftwareID from the table Software.
SupportedEncryptionTypes	NVarchar[255]	Comma separated strings. E.g. "Virtual, Physical, Directory, Archive". Possible values: "Virtual", "Physical", "Directory", "Archive". Note: these values are not translated. These values need to be translated before being displayed.

DiskEncryptionLocations

TABLE NAME:	DiskEncryptionLocations
TABLE DESCRIPTION:	Additional information about the locations on the filesystem which are encrypted using disk encryption software. Collected by OESIS Local.

FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
DiskEncryptionLocationsID	AutoNumber (PK)	PK
DiskEncryptionSoftwareID	Number (FK)	FK to field DiskEncryptionSoftwareID from the table DiskEncryptionSoftware.
LocationName	NVarchar[255]	E.g. “m:”.
EncryptionAlgorithm	NVarchar[255]	“” if location is not encrypted. Other possible values: “AES”, “Blowfish”, “Triple DES”, “CAST”, “AES Diffuser”, “Serpent”, “Twofish”, “AES Twofish”, “AES Twofish Serpent”, “Serpent AES”, “Serpent Twofish AES”, “Twofish Serpent”, etc.
EncryptionKeyLength	Number	The length of the crypto key. Possible values: -1 – N/A.
EncryptionModeOfOperation	Number	-1 – N/A, 0 – unknown, 1 - XTS Mode of Operation. ? Which are the other possible values? // TODO: Ask OPSWAT
EncryptionState	Number	-1 – N/A, 0 – not encrypted, 1 – partially encrypted, 2 – fully encrypted, 3 – disk is a virtual drive, for products which support encryption of physical drives and mounting virtual drives.

DeviceAccessControlSoftware

TABLE NAME:	DeviceAccessControlSoftware	
TABLE DESCRIPTION:	Additional information which is specific to this type of software products. Collected by OESIS Local.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
DeviceAccessControlSoftwareID	AutoNumber (PK)	PK
SoftwareID	Number (FK)	FK to field SoftwareID from the table Software.
ProtectedDevices	NVarchar[255]	Comma separated strings. E.g. “Serial, Parallel, FireWire, USB”. Possible values: “Serial”, “Parallel“, “PCMCIA”, “USB”, “BlueTooth”, “FireWire”, “IrDA”, “WiFi”, “Bus”, “Floppy”, “DVD/CD-ROM”. Note: these values are not translated. These values need to be translated before being displayed.
SupportedDevices	NVarchar[255]	Comma separated strings. E.g. “Serial, Parallel, FireWire, USB”. Possible values: “Serial”, “Parallel“, “PCMCIA”, “USB”, “BlueTooth”, “FireWire”, “IrDA”, “WiFi”, “Bus”, “Floppy”, “DVD/CD-ROM”. Note: these values are not translated. These values need to be translated before being displayed.
IsDeviceControlEnabled	Number	-1 – N/A, 1 – is enabled, 0 – is disabled.

VpnClientSoftware

TABLE NAME:	VpnClientSoftware	
TABLE DESCRIPTION:	Additional information which is specific to this type of software products. Collected by OESIS Local.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
VpnClientSoftwareID	AutoNumber (PK)	PK
SoftwareID	Number (FK)	FK to field SoftwareID from the table Software.
ActiveConnections	Ntext	Comma separated strings. E.g. “Customers, Cyg”.
Profiles	Ntext	Comma separated strings. E.g. “Customers, Cyg”.
VpnType	Number	-1 – N/A, 1 – IPSEC, 2 – SSL, 4 – Mobile VPN.

P2pSoftware

TABLE NAME:	P2pSoftware

TABLE DESCRIPTION:	Additional information which is specific to this type of software products. Collected by OESIS Local.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
P2pSoftwareID	AutoNumber (PK)	PK
SoftwareID	Number (FK)	FK to field SoftwareID from the table Software.
IsRunning	Number	-1 – N/A, 0 – not running, 1 – running.
SupportedNetworks	NVarchar[255]	Comma separated strings. E.g. “Bittorrent, Gnutella2”.

BackupClientSoftware

TABLE NAME:	BackupClientSoftware	
TABLE DESCRIPTION:	Additional information which is specific to this type of software products. Collected by OESIS Local.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
BackupClientSoftwareID	AutoNumber (PK)	PK
SoftwareID	Number (FK)	FK to field SoftwareID from the table Software.

BackupClientSchedule

TABLE NAME:	BackupClientSchedule	
TABLE DESCRIPTION:	Additional information about the schedules from the backup client software. Collected by OESIS Local.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
BackupClientScheduleID	AutoNumber (PK)	PK
BackupClientSoftwareID	Number (FK)	FK to field BackupClientSoftwareID from the table BackupClientSoftware.
ScheduleName	NVarchar[255]	E.g. “Only MySQL”.
DestinationType	NVarchar[255]	Possible values: “CD”, “Folder“, “URL”. Note: these values are not translated. These values need to be translated before being displayed.
Destination	NVarchar[255]	E.g. “c:\SQLBackups”.
LastBackupTime	DateTime	
NextBackupTime	DateTime	

AntivirusSoftware

TABLE NAME:	AntivirusSoftware	
TABLE DESCRIPTION:	Additional information which is specific to this type of software products. Collected by OESIS Local.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
AntivirusSoftwareID	AutoNumber (PK)	PK
SoftwareID	Number (FK)	FK to field SoftwareID from the table Software.
IsRealTimeProtectionEnabled	Number	-1 – N/A, 0 – not enabled, 1 – enabled.
DefinitionFilesDirectories	Ntext	E.g. “c:\Program Data\KAV 10.0\ c:\Program Data\Common\KAV 10.0\”
DefinitionFilesSignatures	NVarchar[255]	E.g. “3297415”. ? //TODO: Ask OPSWAT
DefinitionFilesFileTimestamp	DateTime	
DefinitionFilesVersion	NVarchar[255]	E.g. “200.01.14”.
EngineVersion	NVarchar[255]	E.g. “8.0.0.506”.
LastFullSystemScanTime	DateTime	

AntivirusRecentlyDetectedThreat

TABLE NAME:	AntivirusRecentlyDetectedThreat	
TABLE DESCRIPTION:	Contains the list of threats recently detected by the antivirus software.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
AntivirusRecentlyDetectedThreatID	AutoNumber (PK)	PK
AntivirusSoftwareID	Number (FK)	FK to field AntivirusSoftwareID from the table AntivirusSoftware.
ThreatName	NVarchar[255]	E.g. “W32.Korgo.F”.
ThreatType	Number	Possible values: -1 – N/A, 0 – unknown, 1 – suspicious, 2 – cookie, 3 – virus, 4 – spyware, 5 – Trojan, 6 – adware, 7 – malware.
TimeFound	DateTime	Time when the product identified this threat.
ThreatLocation	NVarchar[255]	Absolute path to the location where threat was found.
ActionTaken	Number	Possible values: -1 – N/A, 0 – No Action was taken. File is still dangerous!, 1 - Threat was deleted, 2- Threat was moved to quarantine zone, 3 - Threat was cleaned. File is safe, 4 - Couldn't determine what action was taken. File may still be dangerous!

AntispywareSoftware

TABLE NAME:	AntispywareSoftware	
TABLE DESCRIPTION:	Additional information which is specific to this type of software products. Collected by OESIS Local.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
AntispywareSoftwareID	AutoNumber (PK)	PK
SoftwareID	Number (FK)	FK to field SoftwareID from the table Software.
IsRealTimeProtectionEnabled	Number	-1 – N/A, 0 – not enabled, 1 – enabled.
DefinitionFilesDirectories	Ntext	E.g. “c:\Program Data\KAV 10.0\ c:\Program Data\Common\KAV 10.0\”
DefinitionFilesSignatures	NVarchar[255]	E.g. “3297415”. ? //TODO: Ask OPSWAT
DefinitionFilesFileTimestamp	DateTime	
DefinitionFilesVersion	NVarchar[255]	E.g. “200.01.14”.
EngineVersion	NVarchar[255]	E.g. “8.0.0.506”.
LastFullSystemScanTime	DateTime	

AntispywareRecentlyDetectedThreat

TABLE NAME:	AntispywareRecentlyDetectedThreat	
TABLE DESCRIPTION:	Contains the list of threats recently detected by the antispyware software.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
AntispywareRecentlyDetectedThreatID	AutoNumber (PK)	PK
AntispywareSoftwareID	Number (FK)	FK to field AntispywareSoftwareID from the table AntispywareSoftware.
ThreatName	NVarchar[255]	E.g. “CoolWebSearch”.
ThreatType	Number	Possible values: -1 – N/A, 0 – unknown, 1 – suspicious, 2 – cookie, 3 – virus, 4 – spyware, 5 – Trojan, 6 – adware, 7 – malware.
TimeFound	DateTime	Time when the product identified this threat.
ThreatLocation	NVarchar[255]	Absolute path to the location where threat was found.
ActionTaken	Number	Possible values: -1 – N/A, 0 – No Action was taken. File is still dangerous!, 1 - Threat was deleted, 2- Threat was moved to quarantine zone, 3 - Threat was cleaned. File

		is safe, 4 - Couldn't determine what action was taken. File may still be dangerous!

FirewallSoftware

TABLE NAME:	FirewallSoftware	
TABLE DESCRIPTION:	Additional information which is specific to this type of software products. Collected by OESIS Local.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
FirewallSoftwareID	AutoNumber (PK)	PK
SoftwareID	Number (FK)	FK to field SoftwareID from the table Software.
FirewallPolicy	NVarchar[255]	
IsEnabled	Number	-1 – N/A, 0 – not enabled, 1 – enabled.

PatchManagementSoftware

TABLE NAME:	PatchManagementSoftware	
TABLE DESCRIPTION:	Additional information which is specific to this type of software products. Collected by OESIS Local.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
PatchManagementSoftwareID	AutoNumber (PK)	PK
SoftwareID	Number (FK)	FK to field SoftwareID from the table Software.
UpdateServerType	Number	Possible values: -1 – N/A, 0 – system default, 1 – managed server, 2 – Windows Update, 3 – server offline.
UpdateServerPath	NVarchar[255]	E.g. http://windowsupdate.microsoft.com.
AgentIsEnabled	Number	-1 – N/A, 0 – not enabled, 1 – enabled.
AutomaticUpdatesStatus	Number	-1 – N/A, 0 – Agent is disabled, 1 - Agent is turned on and will notify user before downloading updates, 2 - Agent is turned on and will notify user before installing updates, 3 - Agent is turned on and will auto update the system.
LastScanTime	DateTime	

UrlFilteringSoftware

TABLE NAME:	UrlFilteringSoftware	
TABLE DESCRIPTION:	Additional information which is specific to this type of software products. Collected by OESIS Local.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
UrlFilteringSoftwareID	AutoNumber (PK)	PK
SoftwareID	Number (FK)	FK to field SoftwareID from the table Software.
IsEnabled	Number	-1 – N/A, 0 – not enabled, 1 – enabled.
LastUpdateTime	DateTime	Retrieves the time of when the client last successfully checked for an update to its URL rule set.

VirtualMachineSoftware

TABLE NAME:	VirtualMachineSoftware	
TABLE DESCRIPTION:	Additional information which is specific to this type of software products. Collected by OESIS Local.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
VirtualMachineSoftwareID	AutoNumber (PK)	PK
SoftwareID	Number (FK)	FK to field SoftwareID from the table Software.

HypervisorType	Number	-1 – N/A, 0 – unknown, 1 – bare metal (the hypervisor is the OS installed directly on the hardware; the hypervisor is not installed on top of an OS, 2 – the hypervisor is installed on top of a host OS (e.g. WMware Workstation installed on top of Windows).

VirtualMachine

TABLE NAME:	VirtualMachine	
TABLE DESCRIPTION:	Contains a list of virtual machines supported by the virtual machine software.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
VirtualMachineID	AutoNumber (PK)	PK
VirtualMachineSoftwareID	Number (FK)	FK to field VirtualMachineSoftwareID from the table VirtualMachineSoftware.
Name	NVarchar[255]	E.g. “”H:\VMs\Development Machine\Windows XP Professional.vmx”.
OSType	Number	Possible values: -1 – N/A, 0 – Unknown, 1 – Linux, 2 – MacOS, 3 – Windows.
OSVersion	NVarchar[255]	
OSDistribution	NVarchar[255]	
CurrentState	Number	Possible values: -1 – N/A, 1 – machine is on/running, 2- machine is paused/suspended, 3 - machine is powered off/stopped.
UserFriendlyName	NVarchar[255]	E.g. “Development Machine”.

VirtualMachineNic

TABLE NAME:	VirtualMachineNic	
TABLE DESCRIPTION:	Contains a list of network interface cards (NICs) for the given virtual machine.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
VirtualMachineNicID	AutoNumber (PK)	PK
VirtualMachineID	Number (FK)	FK to field VirtualMachineID from the table VirtualMachine.
Name	NVarchar[255]	E.g. “Default”.
Type	Number	Possible values: -1 – N/A, 0 – unknown, 1 – NAT, 2 – bridged, 3 – host only, 4 – private.
IsConnected	Number	Possible values: -1 – N/A, 0 – network adapter is not connected, 1 - network adapter is connected, 2- network adapter connection state is unknown.

DataLossPreventionSoftware

TABLE NAME:	DataLossPreventionSoftware	
TABLE DESCRIPTION:	Additional information which is specific to this type of software products. Collected by OESIS Local.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
DataLossPreventionSoftwareID	AutoNumber (PK)	PK
SoftwareID	Number (FK)	FK to field SoftwareID from the table Software.
IsEnabled	Number	-1 – N/A, 0 – data loss prevention is disabled, 1 – data loss prevention is enabled.

InstantMessengerSoftware

TABLE NAME:	InstantMessengerSoftware	
TABLE DESCRIPTION:	Additional information which is specific to this type of software products. Collected by OESIS Local.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
InstantMessengerSoftwareID	AutoNumber (PK)	PK
SoftwareID	Number (FK)	FK to field SoftwareID from the table Software.
ArchivesDirectory	NVarchar[255]	E.g. “C:\Program Files\Yahoo Messenger\Logs”. If Message history tracking were to be enabled, reports the directory in which the conversation data would be stored.
AccountNameOfSignedInUser	NVarchar[255]	E.g. “big2010”. Returns the username of the currently logged in user.
IsMessageArchivingEnabled	Number	-1 – N/A, 0 – the messages that are being received and sent are not saved (archived) , 1 – the messages that are being received and sent are being saved (archived).
SupportedProtocols	NVarchar[255]	E.g. “IRC, Yahoo!, AIM”. //TODO: Ask OPSWAT
IsRunning	Number	-1 – N/A, 0 – IM client is not running, 1 – IM client is running
IsConnected	Number	

Deployments

TABLE NAME:	Deployments	
TABLE DESCRIPTION:	Information about a deployment session performed on one or more targets.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
DeploymentsID	AutoNumber (PK)	PK
DeploymentsType	Number	0 – deploy custom software 1 – deploy MS patches 2 – deploy MS service packs 3 – uninstall MS patches 4 – uninstall MS service packs 5 – uninstall unauthorized applications 6 – autoremediation 7 – deploy non-MS patches 8 – OESIS
ScheduledToStartDateTime	Datetime	Datetime when the session should start running.
CreationDateTime	Datetime	Datetime when the session was ordered.
ScansID	Number	If this remediation is related to a scan session this record points to the record in table Scans which represents the scan session. 0 - if this deployment session has no relation to a scan session.
StartDateTime	Datetime	Datetime when the session started execution.
EndDateTime	Datetime	Datetime when the session’s execution completed.
Enabled	Number	0 – session is not enabled, it should not execute 1 – session is enabled, it should execute
Status	Number	0 – pending 1 – running 2 – rescheduled 4 – complete 5 – completed with errors
Session	Nvarchar[255]	Same as Scans.Session. Session identifier for a deployment session.

DeploymentsStatus

TABLE NAME:	DeploymentsStatus
TABLE DESCRIPTION:	Detailed information about the steps performed to execute the session.

FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
DeploymentsStatusID	AutoNumber (PK)	PK
DeploymentsID	Number(FK)	FK to field DeploymentsID from the table Deployments.
SequenceNo	Number	Aux for sorting.
Message	Nvarchar[255]	Status text (e.g “Downloading notepad.exe”).
StatusType	Number	0 – running 1 – complete 2 – failed

DeploymentsOptions

TABLE NAME:	DeploymentsOptions	
TABLE DESCRIPTION:	Options for a deployment session.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
DeploymentsOptionsID	AutoNumber (PK)	PK
DeploymentsID	Number(FK)	FK to field DeploymentsID from the table Deployments.
LogonType	Number	Well known logon type.
Data1	Nvarchar[255]	GUID for username.
Data2	Nvarchar[255]	GUID for password.
Data3	Nvarchar[255]	GUID for alternative username.
Data4	Nvarchar[255]	GUID for alternative password.
WarnUser	Number	0 – no warning 1 – warn the user 2 – warn the user and wait for approval
StopServices	Number	Stop configured services before deployment.
CustomShare	Nvarchar[255]	Custom share to copy patches to.
RebootAndShutdown	Number	0 – do not reboot or shut down 1 – reboot immediately after deployment 2 – shutdown immediately after deployment 3 – reboot but let the user decide when 4 – reboot at next occurrence of time 5 – shutdown at next occurrence of time 6 – reboot when inside window of time 7 – shut down when inside window of time
DeleteFiles	Number	0 – delete files after deployment 1 – leave files on target
ThreadCount	Number	Number of simultaneous deployment threads.
TimeOut	Number	Seconds to wait for patch agent status messages.
AutodeployMSPatches	Number	Possible values: 0 - no, 1 - yes
AutodeployMSServicePacks	Number	Possible values: 0 - no, 1 - yes
AutodeployNonMSPatches	Number	Possible values: 0 - no, 1 - yes
AutouninstallUnauthorizedApplications	Number	Possible values: 0 - no, 1 – yes
Report_EmailReport	Number	Possible values: 0 - no, 1 – yes
Report_SaveReport	Number	Possible values: 0 - no, 1 – yes
Report_SaveDirectory	Nvarchar[255]	Directory where to save the report.
Report_IncludeFullResults	Number	Possible values: 0 - no, 1 – yes
Report_IncludeComparison	Number	Possible values: 0 - no, 1 – yes
RebootWindowStart	DateTime	We should not reboot/shut down the machine before this time.
RebootWindowEnd	DateTime	We should not reboot/shut down the machine after this time.
ShowRebootCountdown	Int	1 - Should display reboot/shut down countdown dialog, 0 - Otherwise
RebootCountdownSeconds	Int	The number of seconds during which we display the reboot/shut down countdown dialog.
RebootCountdownMessage	Nvarchar(255)	The message shown in the reboot/shut down countdown dialog.
AdvancedOptions	Memo	N/A

Report_ReportID	Nvarchar(255)	The ID of the report to generate.
RebootDays	Nvarchar(255)	We should reboot/shut down the machine only on specified days.
PatchVerificationScan	Number	Possible values: 0 - no, 1 – yes

Deployment

TABLE NAME:	Deployment	
TABLE DESCRIPTION:	Data about a deployment target.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
DeploymentID	AutoNumber (PK)	PK
DeploymentsID	Number(FK)	FK to field DeploymentsID from the table Deployments.
Hostname	Nvarchar[255]	Hostname of the target computer.
IP	Nvarchar[255]	IP address of the target computer.
Mac	Nvarchar[255]	MAC of the target computer.
ComputerID	Number	Points to a record in the Computer table by ComputerID but it is not a FK.
Status	Number	0 – pending, awaiting start 1 – completed successfully 2 – completed with errors 3 – errors encountered while executing deployment on this computer 4 – timeout 5 – rescheduled for later because it was not found online
Error	Nvarchar[255]	Error text in case of failure.
RebootRequired	Number	0 – reboot is not required 1 – reboot is required

DeploymentStatus

TABLE NAME:	DeploymentStatus	
TABLE DESCRIPTION:	Detailed information about the steps performed on each target.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
DeploymentStatusID	AutoNumber (PK)	PK
DeploymentID	Number(FK)	FK to field DeploymentID from the table Deployment.
SequenceNo	Number	Aux for sorting and sequencing async messages.
Message	Nvarchar[255]	Text for the operation.
StatusType	Number	0 – running 1 – complete 2 – failed

DeploymentDetail

TABLE NAME:	DeploymentDetail	
TABLE DESCRIPTION:	Info about each remediation operation that is to be performed.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
DeploymentDetailID	AutoNumber (PK)	PK
DeploymentID	Number(FK)	FK to field DeploymentID from the table Deployment.
DeploymentDetailType	Number	0 – NA 1 – patch install 3 – application uninstall 4 – custom software 5 – patch uninstall 7 – auxiliary file 8 – OESIS
FileLocation	Memo	Path to the file.

RemoteName	Nvarchar[255]	Name of the file when copied to target.
CommandLineSwitches	Memo	Command line switches for the deployment operation.
FullCommandLine	Memo	Full command line of the operation.
BulletinID	Nvarchar[255]	Bulletin ID for a patch.
Name	Nvarchar[255]	Name (KB article ID) for a patch.
Title	Memo	Title for a patch.
FileName	Nvarchar[255]	File name for a patch.
FileSize	Nvarchar[255]	Size of the file in bytes.
FileDigest	Nvarchar[255]	Digest of the file.
FileDownloadUri	Memo	URL where a file can be downloaded from.
Language	Nvarchar[255]	Language for a patch.
DatePosted	Nvarchar[255]	Date when a patch was posted.
MoreInfoUri	Memo	Where to find more information.
Status	Number	0 – pending 1 – completed 2 - downloading
Severity	Nvarchar[255]	Patch severity. Not translated. Possible values: "", "Critical", "Important", "Moderate", "Low".
AddressesIssue	Number	Possible values: 0 - is not fixing a vulnerability or a policy issue (e.g. custom sotware deployment, manual uninstallation of an application etc.), 1 - is fixing a vulnerability or a policy issue (e.g. uninstallation of an unauthorized application).
UpdateType	Nvarchar[255]	Possible values: 5 - Security Updates, 6 - Critical Updates, 7 – Updates, 8 - Update Rollups, 9 - Service Packs, 10 - Feature Packs.
AppliesToCategory	nvarchar[255]	Specifies the category of products the update applies to.
RebootRequired	Number	0 – reboot is not required 1 – reboot is required
ErrorCode	Number	Error code returned by patch installation
ErrorMessage	Memo	Message of error code returned by patch installation
DetailStatus	Number	Detail Status of the deployment(pending, success, download failed, execution error etc.)

ApplicationUserSession

TABLE NAME:	ApplicationUserSession	
TABLE DESCRIPTION:	Stores information about multiple sessions from LGW console.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
ApplicationUserSession ID	AutoNumber (PK)	PK
SessionCookie	Nvarchar[255]	Value of the identification Cookie obtained from browser.
TimeStamp	DateTime	The date and time this session has been created.

CentralManagementAgent

TABLE NAME:	CentralManagementAgent	
TABLE DESCRIPTION:	Contains a list of all the product installations which are agents of this Central Management Console.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
CentralManagementAgentID	AutoNumber (PK)	PK
CentralManagementAgentUid	Text	
Name	Text	
Location	Text	Address.
LicensedNumberOfNode	Number	

s		
LicenseHash	Number	
RemainingLicensesNodes	Number	
IsTrialLicense	Number	
TotalNumberOfNodes	Number	
LicenseExpiryDate	Date	
Latitude	Double	
Longitude	Double	
Description	Text	
InstallationID	Text	
TimestampOfFullDataRequest	DateTime	Used in db change

ComputerToCentralManagementAgent

TABLE NAME:	ComputerToCentralManagementAgent	
TABLE DESCRIPTION:	Used to link computers from the database to the groups they belong to.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
ComputerToCentralManagementAgentID	AutoNumber (PK)	PK
ComputerID	Number (FK)	The ID of the computer.
CentralManagementAgentID	Number (FK)	The ID of the central management agent.

ComputerCentralManagement_Agent

TABLE NAME:	ComputerCentralManagement_Agent	
TABLE DESCRIPTION:	LANSS only. Details of pushing data from LANSS to LGCMC for a computer.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
ComputerCentralManagement_AgentID	AutoNumber (PK)	PK
ComputerID	Number (FK)	ID of the computer where the security scanner agent runs.
TimestampOfFullComputerDataRequest	Date	Date when LGCMC has requested resending full data about this computer.
TimestampOfFullDataExport	Date	Date when we have last exported full data for this computer.

ComputerCentralManagement_Server

TABLE NAME:	ComputerCentralManagement_Server	
TABLE DESCRIPTION:	LGCMC only. Details of receiving data in LGCMC from LANSS for a computer.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
ComputerCentralManagement_ServerID	AutoNumber (PK)	PK
ComputerID	Number (FK)	ID of the computer where the security scanner agent runs.
TimestampOfComputerDataError	Date	Date when the central management server found invalid checksum for data for this computer.

Vulnerability

TABLE NAME:	Vulnerability	
TABLE DESCRIPTION:	The Vulnerability table contains the vulnerability that were found on scanned machines.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
VulnerabilityID	AutoNumber (PK)	PK
Name	nvarchar[255]	Contains name of vulnerability.
Type	nvarchar[255]	Alert type has the following possible values: 'FTP', 'Mail', 'RPC', 'Services', 'DNS', 'Information', 'Miscellaneous', 'Registry', 'Black listed network devices', 'Black listed USB devices', 'Unauthorized applications', 'Security products', 'Software', 'Web', 'Rootkit', 'Malware protection', 'Firewall'. Note: do not translate.
Description	Memo	Description of the vulnerability.
Bugtraq	nvarchar[255]	Id of the alert or URL to a web page that contains detailed explanation of the alert.
Level	Int	Level of severity, possible values: 0 - High, 1 - Medium, 2 - Low, 3 - Potential.
Product	nvarchar[255]	Name of the affected product.
OVAL_ID	nvarchar[255]	ID for the security database OVAL.
CVE_ID	nvarchar[255]	ID for the security database CVE.
MS_Security_BID	nvarchar[255]	ID for the security database Microsoft.
Security_Focus_BID	nvarchar[255]	ID for the security database Security Focus.
Timestamp	nvarchar[255]	Timestamp when the entry was created.
TopSansYear	nvarchar[255]	The year in which the current patch was in the SANS organization vulnerabilities top.
TopSansChapter	nvarchar[255]	The name of the SANS organization vulnerabilities top in which the current patch was positioned in the year represented by the above mentioned field. Note: do not translate.
CVSS_Score	Numeric(18,2)	Severity score extracted from CVE dabase.

VulnerabilityToScan

TABLE NAME:	VulnerabilityToScan	
TABLE DESCRIPTION:	There are found relationships between vulnerabilities and Scan.	
FIELD NAME:	FIELD TYPE	FIELD DESCRIPTION
VulnerabilityToScanID	AutoNumber (PK)	PK
VulnerabilityToScanUid	nvarchar[36]	Uid of the entry.
VulnerabilityID	Number (FK)	ID of the found vulnerability.
ScanID	Number (FK)	ID of the scan when vulnerability was found.
Error	nvarchar[255]	Description of the error if there was an error.
Status	Int	1 if there was an error retrieving data, 0 otherwise.
Hash	nvarchar[40]	Hash of the row.
ComputerUid	nvarchar[36]	Uid of the computer on which vulnerability was found.