Product Specification

SekChek Local: SAM

First Published: August, 2008
Last Revision: January, 2013

inbox@sekchek.com
www.sekchek.com

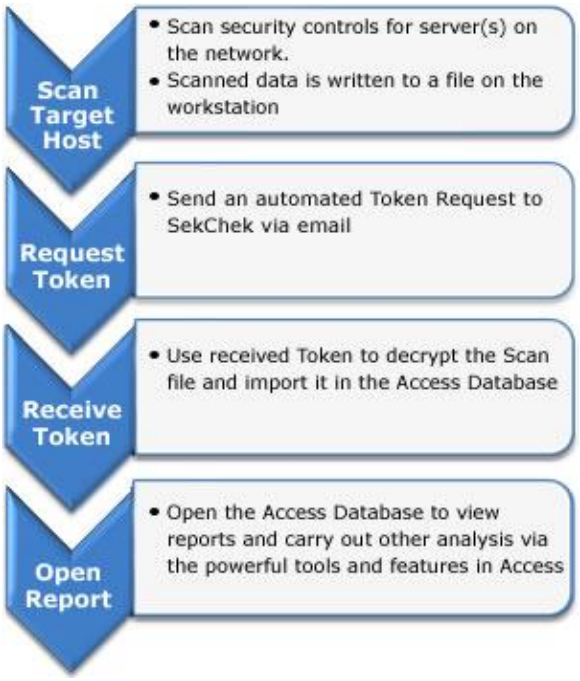
Contents

1. Main Features

The Local SAM tool analyses *local* security policies and objects defined on one or more member computers. It supports all business versions of Microsoft Windows, including Windows NT, 200X and Vista.

Note that the SAM tool does not support systems running Active Directory (i.e. Win200X Domain Controllers). If your objective is to analyse an Active Directory domain you should use the Local AD tool because it caters for the richer set of objects and properties defined in Active Directory databases.

The Local SAM Tool…

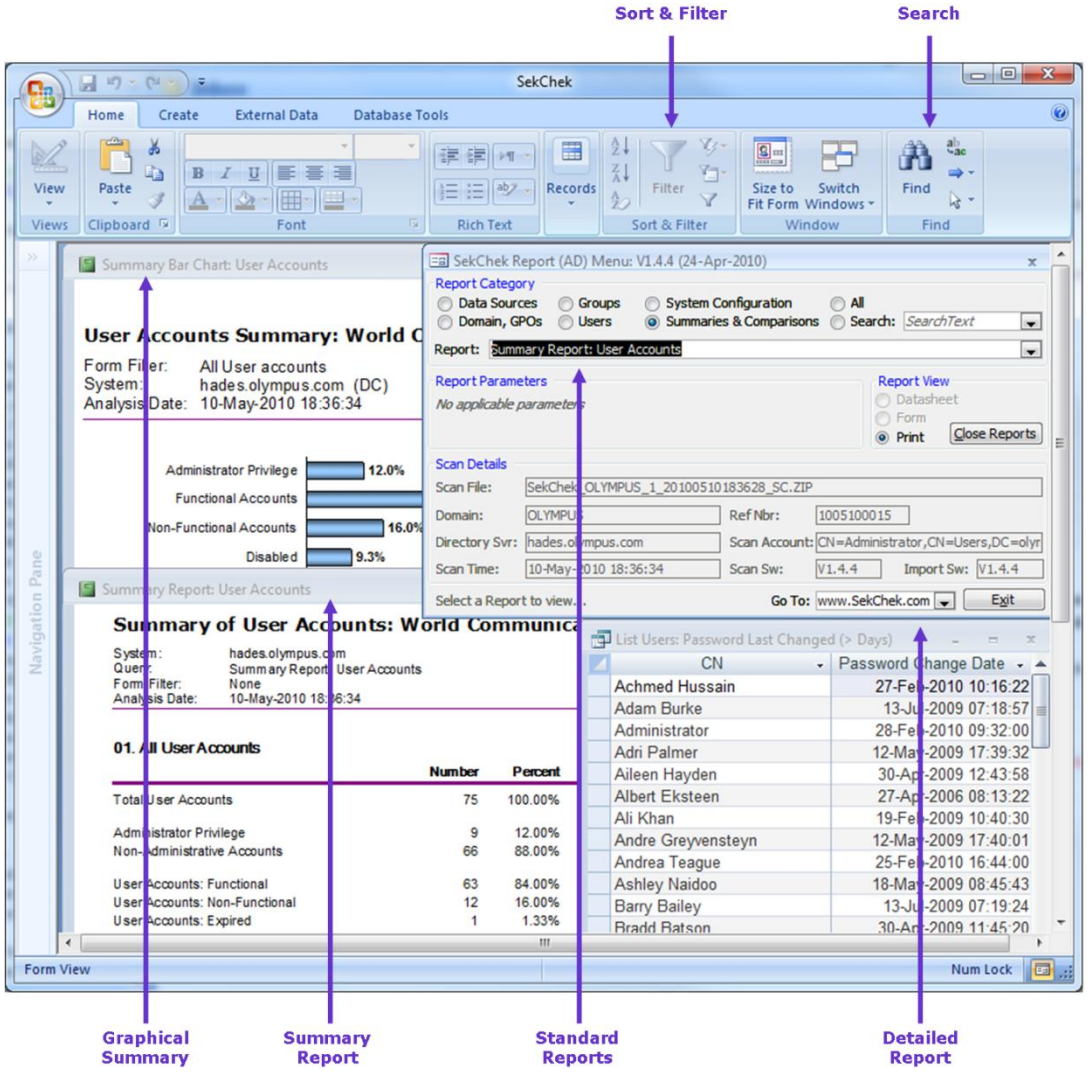


- Analyses security on any Windows Server from a single point on the network
- Analyses multiple Servers in a single Scan
- Compares security policies against real-life industry averages and leading practices for security
- No data leaves your organisation... Scan files are processed locally on your PC
- Consistent, objective and comprehensive reporting... not sample-based
- Provides a comprehensive set of standard reports, including detailed and summary views
- Report data can be queried, sorted, copied / pasted, graphed & printed
- No software is installed, or executed on the target Host system… the processing is done over the network from a regular workstation... no impact on the Host system.
- Fast turnaround time… Scans take only a few minutes to run... Access Tokens are issued immediately on receipt of your Token request.
- Economical… no software licensing fees… you pay only when you use the tool.

SekChek Local provides you with:

- A Report Database in MS-Access format containing a collection of predefined summary, graphical, and detailed reports. SekChek's standard reports provide answers to the most common questions on security.
- Access to powerful data manipulation and query utilities, which means you can develop your own customised reports and queries.
- Software that allows you to analyse multiple Hosts in a single Scan. The software runs on a workstation connected to your network.
- A family of useful utilities, including: File encryption / decryption tools; a file hashing function; a tool that queries 'hidden' properties on security accounts; and a 'Ping' function for testing network connectivity.

The Report Database provides you with the power and flexibility you need to view and analyse security in a variety of ways.



For example, you can elect to use SekChek's predefined reports or to analyse data directly within the Access environment. Standard reports consist of detailed exception reports and easy-to-read summary reports.

Both options allow you to use familiar data manipulation functions, such as the Sorting, Searching and Filtering of records. You can even create Pivot tables and graphs, which allow you to create complex, customised views and charts.

Finally, regardless of which option you choose you can work on a single Scan file, a subset of Hosts, or all Scanned Hosts. This means you can quickly compare security settings across a number of different systems.

2. Summary of Reports & Analyses

SekChek's predefined reports provide quick answers to common questions about security, for example:

- Which Users defined on Host X have not changed their password in the last 90 days?
- What system events are being audited on Host Y?
- Which Hosts do not comply with your standards for password change frequency or minimum password length?
- What is the percentage of accounts with Administrator / User / Guest privileges?
- What permissions and auditing controls are defined on key system directories?
- Which accounts have powerful rights, such as the ability to shutdown the system?

Familiar selection boxes allow you to select a Report and quickly scroll through a series of Hosts, or display high level summary reports that include information for all Hosts.

The following tables summarise the standard reports provided with the SAM product. The remainder of the document provides a detailed and comprehensive list of the security objects and attributes included in the Local SAM Report Database.

Effective Policies

Report Description	Detailed	Summary
Password Policies	X	X
Account Lockout Policies	X	X
Audit Policies	X	X
Force Logoff Policy	X	X
Administrator / Guest Account Status	X	X
Rename Administrator / Guest Policies	X	X

User Accounts

Report Description	Detailed	Summary
Administrative Accounts	X	X
All User Accounts	X	X
Cannot Change Password	X	X
Duplicate SAM Accounts	X	
Functional Accounts	X	X

User Accounts

Report Description	Detailed	Summary
Last Logon > 30 / 60 / 90 / 180 / 360 Days	X	X
Last Logon Never	X	X
Logon Hours Unrestricted	X	X
Non-Functional Accounts	X	X
Password Expired	X	X
Password Last Changed > 30 / 60 / 90 / 180 / 360 Days	X	X
Password Last Changed Never	X	X
Password Never Expires	X	X
Password Not Required	X	X
Password Stored with Reversible Encryption	X	X
Smart Card Required	X	X

Group Accounts

Report Description	Detailed	Summary
All Security Groups	X	X
Duplicate Group Accounts	X	
Global Groups		X
Group Members	X	
Groups with no Members	X	X
Local Groups		X

System Configuration

Report Description	Detailed	Summary
Base Board	X	X
BIOS	X	X
Computer Config	X	X
Disk Drives	X	X
Host Roles	X	X

Report Description	Detailed	Summary
Hot Fixes Installed	X	X
Network Adapters	X	X
Network Shares	X	X
Operating System	X	X
OS Recovery Options	X	X
Page Files	X	X
Processors	X	X
Products Installed [from V1.4.5]	X	X

Other Reports

Report Description	Detailed	Summary
Account Privileges	X	X
Directory Auditing (SACLs)	X	
Directory Permissions (DACLs)	X	
Event Log Settings	X	
Host Properties	X	
Security Options	X	
Services	X	X

3. Detailed List of Attributes Analysed

The following tables provide a complete list of attributes – by data group - scanned by the SAM product.

Account Right Properties

Account Name	The name of the account with the privilege.
Account Type	The type of account. E.g. User, Group, Alias, WellKnownGroup.
Domain	The domain (or computer) where the account is defined.
Privilege	The privilege assigned to the account.
Well-known Name	The well-known name for the account. E.g. BUILTIN, NT AUTHORITY.

Audit Event Properties

Account Logon Events	Audit logon attempts by privileged accounts that log on to the domain controller. These audit events are generated when the Kerberos Key Distribution Center logs on to the domain controller.
Account Management	Audit attempts to create, delete, or change user or group accounts. Also, audit password changes.
Auditing Mode	Indicates whether auditing is enabled. If enabled, the system generates audit records according to the event auditing options specified.
Directory Service Access	Audit attempts to access the directory service.
Logon Events	Audit attempts to log on to or log off from the system. Also, audit attempts to make a network connection.
Object Access	Audit attempts to access securable objects, such as files.
Policy Change	Audit attempts to change Policy object rules.
Privilege Use	Audit attempts to use Windows privileges.
Process Tracking	Audit events such as program activation, some forms of handle duplication, indirect access to an object, and process exit.
System Events	Audit attempts to shut down or restart the computer. Also, audit events that affect system security or the security log.

Base Board Properties

Manufacturer	The manufacturer of the baseboard (motherboard / system board)
Product	The product name or part number
Serial Number	Manufacturer-allocated number used to identify the component
Version	Version number assigned by the manufacturer

BIOS Properties

Bios	Description of the BIOS
Manufacturer	The manufacturer of the BIOS
Release Date	Release date of the Windows BIOS (YYYY-MM-DD)
Version	BIOS version (Major.Minor)

Computer Properties

Allow Remote Desktop	Indicates whether new Terminal Services connections are allowed. (from Win 2003) [from V1.4.2]
Boot ROM Supported	Indicates whether the system supports a boot ROM
Bootup State	Boot-up mode. E.g. Normal boot, Fail-safe boot.
Domain	The name of the domain to which the computer belongs
Domain Role	The role of the computer in an assigned domain workgroup
Infrared Port Exists	Indicates whether an infrared (IR) port exists on the system
Manufacturer	Manufacturer of the computer
Model	Product name assigned by the manufacturer
Nbr Processors	The number of enabled processors that are currently available on the system
Power Mgt Supported	Indicates whether the system supports power-management
System Type	The type of system running on the computer. E.g. X86-based PC, 64-bit Intel PC
Total RAM (GB)	The total size of physical memory on the system. Expressed in gigabytes
Wakeup Type	Event that causes the system to power up

Disk Properties

ACLs	Indicates whether the file system preserves and enforces access control lists (ACL).
Capacity (GB)	The size of the drive in gigabytes.
Case Is Preserved	Indicates whether the file system preserves the case of file names when it places a name on disk.
Case Sensitive	Indicates whether the file system supports case-sensitive file names.
Compressed Volume	Indicates whether the volume is a compressed volume.
Disk Quotas	Indicates whether the file system supports disk quotas.
Drive	The drive letter. Range: A-Z.
Drive Type	The type of drive. E.g. 3 1/2 Inch Floppy Drive, Local Fixed Disk.
File Compression	Indicates whether the file system supports file-based compression.
File Encryption	Indicates whether the file system supports the Encrypted File System (EFS).

File System	The file system type. E.g. FAT, NTFS
Free Space %	Percentage of free space available on the drive.
Free Space (GB)	The free space on the drive in gigabytes.
Max Component Length	The maximum length of a file name component supported by the file system. A file name component is the portion of a file name between backslashes.
Named Streams Supported	Indicates whether the file system supports named streams.
Read Only	Indicates whether the volume is mounted as read-only.
Re-Parse Points Supported	Indicates whether the file system supports re-parse points.
Sequential Write Once Supported	Indicates whether the volume supports a single sequential write.
Serial Number	The volume serial number.
Sparse Files Supported	Indicates whether the file system supports sparse files.
Transactions Supported	Indicates whether the volume supports transactions.
Unicode Supported	Indicates whether the file system supports Unicode in file names as they appear on disk.
Volume Name	An optional description of the drive.

Event Log Properties

Application Log: File Name	The location of the event log file
Application Log: Max Size (KB)	The maximum size of the log file (KB)
Application Log: Retention Method	The retention method. E.g. Overwrite events as needed (dependent on Max Size), Overwrite events older than XX days.
Application Log: Retention Period (days)	The number of days records are retained before being overwritten
Security Log: File Name	The location of the event log file
Security Log: Max Size (KB)	The maximum size of the log file (KB)
Security Log: Retention Method	The retention method. E.g. Overwrite events as needed (dependent on Max Size), Overwrite events older than XX days.
Security Log: Retention Period (days)	The number of days records are retained before being overwritten
System Log: File Name	The location of the event log file
System Log: Max Size (KB)	The maximum size of the log file (KB)
System Log: Retention Method	The retention method. E.g. Overwrite events as needed (dependent on Max Size), Overwrite events older than XX days.
System Log: Retention Period (days)	The number of days records are retained before being overwritten

Group Member Properties

Account Type	The account type of the member. E.g. User, Group, WellKnownGroup
Group Name	The name of the group.
Group Type	The type of Group: Global or Local.
Member	The account name of the group member. For a Local group the member can be a user or a global group account.
Member Domain	The domain (or computer) to which the group member belongs.
Well-known Name	E.g. NT AUTHORITY

Group Properties

Comment	A remark associated with the group.
Group Id	The relative identifier of the global group.
Group Name	The name of the group.
Group Type	The type of Group: Global or Local.
Redundant?	If 'Yes', the group does not contain any members.

Host Properties

Client Machine	The machine from which the Scan was run
Domain Name	The Host's domain (or workgroup)
Force Logoff	The number of seconds between the end of the valid logon time and the time when the user is forced to log off. -1: never forced to log off. 0: forced to log off immediately when the valid logon time expires.
Host IP Address	The Host's IP Address. E.g. 224.100.200.5 [from V1.4.4]
Hostname	The name of the Host that was scanned
Hostname (DN)	The Host's Distinguished Name (DN). E.g. CN=MyHost,DC=research,DC=sekchek,DC=com [from V1.4.4]
Hostname (DNS)	The Host's DNS name. E.g. MyHost.research.sekchek.com [from V1.4.4]
Locale Id: Client System	The client system's Locale Id
Locale Id: User	The user's Locale Id
Lockout Duration	The time in minutes that a locked account remains locked before it is automatically unlocked. 0 = lockout indefinitely (until the account is unlocked by an Administrator)
Lockout Observation Window	The maximum time, in minutes, that can elapse between the number of failed logon attempts defined in Lockout_Threshold before lockout occurs.
Lockout Threshold	The number of invalid password authentications that can occur before an account is 'locked'.
Max Password Age	The maximum number of days allowed between password changes
Min Password Age	The minimum number of days allowed between password changes
Min Password Length	The minimum allowed password length

OS Build Nbr	The build number of the OS on the Host
OS Version	The version of Windows running on the Host
Password Complexity	The password must have a mix of at least two of the following types of characters: upper case; lower case; numerals
Password History Length	The number of previous passwords remembered by Windows (prevents passwords from being cycled)
Reversible Passwords	The user's password is stored under reversible encryption in the Active Directory (XP & later)
Role	The role of the Host (Domain Controller, Server, Workstation)
Scan Account	The account used to perform the Scan
Scan Time	The time that the Host was Scanned
Service Pack	The Window's Service Pack installed on the Host
SID: Domain	Security Identifier (SID) for the domain.
SID: Server	Security Identifier. If the Server is a DC, it is the SID for the domain. For non-DCs it is the SID of the Server.
Time Zone Bias	The time zone bias, relative to GMT, on the machine where the Scan was run

Host Roles

Alternate Transport	Alternative transport
Apple File Protocol	Apple File Protocol server
Backup Browser	Server running a Browser service as backup
Backup DC	Backup Domain Controller
Cluster Server	Server cluster
Cluster Virtual Server	Cluster virtual server
DFS Root	Root of a DFS tree
Dial-in Server	Server running dial-in service
Domain Master Browser	Server running the domain master Browser
Domain Member	LAN Manager 2.x domain member
File & Print for Netware	Microsoft File and Print for Netware
IBM DSS	IBM DSS (Directory and Security Services) or equivalent
Local List	Servers maintained by the Browser / Return local list only
Master Browser	Server running the master Browser service
Novell Server	Novell Server
OSF Server	OSF Server
Potential Browser	Server that can run the Browser service
Primary DC	Primary Domain Controller
Primary Domain	Primary domain

Print Server	Server sharing print queue
Server Service	A LAN Manager server
SQL Server	Any server running with MS SQL Server
Terminal Server	Terminal Server
Time Source	Server running the Timesource service
UNIX Server	Xenix server / UNIX
VMS Server	VMS Server
Windows 95 (or later)	Windows Me, Windows 98 or Windows 95
Windows for Workgroups	Server running Windows for Workgroups
Windows NT (or later)	Windows Server 2003, XP, 2000 or NT
Windows Server (non-DC)	Windows Server 2003, 2000 ot NT that is not a Domain Controller
Workstation	A LAN Manager workstation

Hot Fixes Installed on the System

Description	Description of the update
Install Date	The date that the update was installed
Installed By	Person who installed the update
Update Id	Unique identifier associated with the Quick Fix Engineering (QFE) update

Network Adapters

Adapter Type	Network medium in use.
Connection Status	State of the network adapter's connection to the network. This property is new for Windows XP.
Default IP Gateway	The IP addresses of default gateways that the computer system uses.
Description	The name of the current network adapter.
DHCP Enabled	Indicates whether the dynamic host configuration protocol (DHCP) server automatically assigns an IP address to the computer system when establishing a network connection.
DHCP Lease Expires	Expiration time for a leased IP address that was assigned to the computer by the DHCP server.
DHCP Lease Obtained	The time the lease was obtained for the IP address assigned to the computer by the DHCP server.
DHCP Server	IP address of the dynamic host configuration protocol (DHCP) server.
DNS Domain	Organization name followed by a period and an extension that indicates the type of organization, such as sekchek.com.
DNS Domain Suffix Search Order	Array of DNS domain suffixes to be appended to the end of host names during name resolution. [from V1.3.9]
DNS Enabled for WINS	Indicates whether DNS is enabled for name resolution over WINS resolution. If the name cannot be resolved using DNS, the name request is forwarded to WINS for

	resolution. [from V1.3.9]
DNS Host Name	Host name used to identify the local computer for authentication by some utilities. [from V1.3.9]
DNS Svr Search Order	Server IP addresses used for querying DNS servers.
Domain DNS Registration Enabled	Indicates whether the IP addresses for this connection are registered in DNS under the domain name of this connection in addition to being registered under the computer's full DNS name. Introduced in Windows XP. [from V1.3.9]
Enable LMHOSTS Lookup	Indicates whether local lookup files are used for WINS. Lookup files will contain a map of IP addresses to host names. [from V1.3.9]
Full DNS Registration Enabled	Indicates whether the IP addresses for this connection are registered in DNS under the computer's full DNS name. Introduced in Windows XP. [from V1.3.9]
Index	Index number of the Windows network adapter configuration.
IP Address	The IP addresses associated with the current network adapter.
IP Enabled	Indicates whether TCP/IP is bound and enabled on this network adapter.
IP Filter Security Enabled	Indicates whether IP port security is enabled globally across all IP-bound network adapters and whether the security values associated with individual network adapters are in effect. [from V1.3.9]
IP Subnet	The subnet masks associated with the current network adapter.
Last Reset	Date and time the network adapter was last reset.
MAC Address	Media Access Control (MAC) address of the network adapter. A MAC address is assigned by the manufacturer to uniquely identify the network adapter.
Manufacturer	Name of the network adapter's manufacturer.
Network Connection Name	Name of the network connection as it appears in the Network Connections Control Panel program.
Service Name	Service name of the network adapter.
Speed (Mbs)	Estimate of the current bandwidth in Megabits per second. Introduced in Windows Vista / 2008.
TCP/IP NetBios Setting	Shows the settings related to NetBIOS over TCP/IP (NetBT). Introduced in Windows XP. [from V1.3.9]
WINS LMHOSTS File	Path to a WINS lookup file on the local system. This file will contain a map of IP addresses to host names. [from V1.3.9]
WINS Primary Svr	IP address for the primary WINS server. [from V1.3.9]
WINS Scope Id	Value appended to the end of the NetBIOS name that isolates a group of computer systems communicating with only each other. It is used for all NetBIOS transactions over TCP/IP communications from that computer system. [from V1.3.9]
WINS Secondary Svr	IP address for the secondary WINS server. [from V1.3.9]

Operating System Properties

Boot Device	The name of the disk drive from which the Windows OS boots. E.g. \\Device\Harddisk0
Country Code	Code for the country/region that an OS uses. Values are based on international phone dialing prefixes.
DEP Available	Indicates whether the Data Execution Protection (DEP) feature is available.

	On 64-bit computers, the data execution prevention feature is configured in the BCD store. (from Win2008) [from V1.4.5]
DEP Drivers	If the DEP hardware feature is available, it indicates whether the feature is set to work for drivers. On 64-bit computers, the DEP feature is configured in the BCD store. (from Win2008) [from V1.4.5]
DEP Enabled (32 bit appls)	If the data execution prevention (DEP) hardware feature is available, indicates whether it is set to work for 32-bit applications. On 64-bit computers, DEP is configured in the Boot Configuration Data (BCD) store. (from Win2008) [from V1.4.5]
DEP Policy	Indicates which DEP setting is applied. The DEP setting specifies the extent to which DEP applies to 32-bit applications. DEP is always applied to the Windows kernel. (from Win2008) [from V1.4.5]
Encryption Level	Encryption level for secure transactions (Windows 2000 & later). E.g. 40-bit, 128-bit
Free RAM (GB)	Number of gigabytes of physical memory currently unused and available.
Installed	The date that the OS was installed
Last Bootup	Indicates when the OS was last booted
Max Processes	Maximum number of process contexts the operating system can support. 0 = unlimited. [from V1.4.5]
Nbr Current Users	The number of user sessions for which the operating system is storing state information currently [from V1.4.5]
Nbr Licenses Users	The number of user licenses for the operating system. 0 = unlimited. [from V1.4.5]
OS Language	Language version of the operating system installed
OS Locale	Language used by the operating system
OS SKU Name	Stock Keeping Unit (SKU) name for the operating system (from Win2008) [from V1.4.2]
OS Name	Short description of the Operating System
PAE Enabled	Indicates whether the Physical Address Extension (PAE) is enabled by the OS running on Intel processors. PAE allows applications to address more than 4 GB of physical memory
Registered User	Name of the registered user of the operating system [from V1.4.5]
Serial Nbr	OS serial identification number
System Directory	System directory of the operating system. E.g. C:\Windows\System32
System Drive	Letter of the disk drive on which the OS resides. E.g. C:
Time Zone Bias	The time zone bias, relative to GMT, on the Host/target system
Visible RAM (GB)	Total amount of physical memory available to the OS. This value does not necessarily indicate the true amount of physical memory.
Windows Directory	Windows directory of the OS. E.g. C:\Windows

OS Recovery Options [from V1.4.2]

Auto Reboot	Indicates whether the system will automatically reboot during a recovery operation.
Debug File Path	Path to the debug file. A debug file is created with the memory state of the computer after a computer failure.
Debug Info Type	The type of debugging information written to the log file. (from Win 2003)
Overwrite Existing Debug File	Indicates whether a new log file will overwrite an existing one.
Send Admin Alert	Indicates whether alert message will be sent to the system administrator in the event of an operating system failure.
Write to System Log	Indicates whether events will be written to a system log.

Page File Properties

Allocated Size (GB)	The amount of disk space (in gigabytes) allocated for use with this page file
Created	When the page file was created
Current Usage (GB)	The amount of disk space (in gigabytes) currently used by the page file
Page File	Name of the page file. E.g. C:\pagefile.sys
Peak Usage (GB)	The highest use (in gigabytes) of the page file
Temporary	Indicates whether a temporary page file has been created, usually because there is no permanent page file on the system

Permissions Properties

Account	The name of the account to which this ACE applies.
Account Type	The type of the account. E.g. Alias, User, Group.
Ace Nbr	Window's reads ACEs in this order until it finds a Deny or Allow ACE that denies or permits access to the resource or an Audit ACE that defines what is audited and the event type.
Ace Type	Allow or Deny access to the resource in the case of an ACE in a DACL; Success or Fail events for a SACL.
ACL Type	The type of ACL being analysed: a DACL or a SACL.
Apply Onto	Specifies where permissions or auditing are applied. These values are shown as they appear in the Windows' property box. E.g. This folder, subfolders & files
Change Permissions	Allows or denies changing permissions of the file or folder, such as Full Control, Read, and Write.
Create Files / Write Data	Create Files allows or denies creating files within the folder. Write Data allows or denies making changes to the file and overwriting existing content (applies to files only).
Create Folders / Append Data	Create Folders allows / denies creating folders within the folder. Append Data allows / denies making changes to the end of the file but not changing, deleting, or overwriting data.
Delete	Allows or denies deleting the file or folder. If you don't have Delete permission on a file or folder, you can still delete it if you have Delete

	Subfolders and Files on the parent folder.
Delete Subfolders And Files	Allows or denies deleting subfolders and files, even if the Delete permission has not been granted on the subfolder or file. (applies to folders)
Domain	The account's domain.
File Synchronise	Allows or denies different threads to wait on the handle for the file or folder and synchronize with another thread that may signal it.
Inherited	Indicates whether the permissions or audit settings are inherited from a higher level.
List Folder / Read Data	List Folder allows or denies viewing file names and subfolder names within the folder. Read Data allows or denies viewing data in files (applies to files only).
Owner	The owner of the resource.
Owner Account Type	The owner's account type. E.g. Alias, User.
Owner Domain	The resource owner's domain.
Read Attributes	Allows or denies viewing the attributes of a file or folder, such as read-only and hidden. Attributes are defined by NTFS.
Read Extended Attributes	Allows or denies viewing the extended attributes of a file or folder. Extended attributes are defined by programs and may vary by program.
Read Permissions	Allows or denies reading permissions of the file or folder, such as Full Control, Read, and Write.
Resource Name	The name of the resource being analysed.
Resource Type	The type of resource being analysed.
Special Permissions	Any other combination of specific permissions.
Take Ownership	Allows or denies taking ownership of the file or folder. The owner of a file or folder can always change permissions on it, regardless of any permissions that protect the file or folder.
Traverse Folder / Execute File	Traverse Folder allows or denies moving through folders to reach other files or folders, even if the user has no permissions for the traversed folders. Execute files.
Write Attributes	Allows or denies changing the attributes of a file or folder, such as read-only or hidden. Attributes are defined by NTFS.
Write Extended Attributes	Allows or denies changing the extended attributes of a file or folder. Extended attributes are defined by programs and may vary by program.

Processor Properties

Address Width	Processor address width in bits
Chip Socket	Type of chip socket used on the circuit. E.g. J202
Clock Speed (MHz)	Current clock speed in MegaHertz
Data Width	Processor data width in bits
Description	E.g. x86 Family 15 Model 2 Stepping 9
Device Availability	Availability and status of the device. E.g. Running/Full Power

External Clock Speed (MHz)	External clock speed in MegaHertz
Family	Processor family type. E.g. Intel® Xeon™
L2 Cache Size (KB)	Size of the Level 2 processor cache in Kilobytes
L2 Cache Speed (MHz)	Clock speed of the Level 2 processor cache in MegaHertz
Manufacturer	Name of the processor manufacturer. E.g. GenuineIntel
Name	Label by which the object is known. E.g. Intel(R) Pentium(R) 4 CPU 2.80GHz
Nbr	Processor Number
Nbr Cores	Number of processor cores. (not supported for Win 2003, XP, 2000)
Nbr Logical Processors	Number of logical processors. (not supported for Win 2003, XP, 2000)
Power Mgt Supported	Indicates whether the power of the device can be managed
Processor Architecture	Processor architecture that the platform uses. E.g. x86, IPF
Processor Id	Processor information that describes the processor features. E.g. BFEBFBFF00000F29
Processor Status	Current status of the processor. E.g. CPU Enabled
Processor Type	Primary function of the processor. E.g. Central Processor
Role	Processor role. E.g. Central Processor
Unique Processor Id	Unique identifier of a processor on the system. E.g. CPU0

Products Installed [from V1.4.5]

Install Date	Product installation date (YYYY-MM-DD)
Install Location	Location of the installed product
Package Location	Location of the locally cached package for this product
Product Id	The product ID
Product Name	The name of the product. Only products installed with the MSI provider (Windows Installer provider) are listed
Publisher	Name of the product supplier
Version	Product version information

Security Options Properties

Accounts: Administrator account status	Indicates whether the Administrator account has been disabled
Accounts: Guest account status	Indicates whether the Guest account has been disabled
Accounts: Rename administrator account	Indicates whether the Administrator account has been renamed
Accounts: Rename guest account	Indicates whether the Guest account has been renamed
Audit: Audit the use of global system objects	Audit the use of global system objects.

Audit: Shut down system immediately if unable to log security audits	Shut down system immediately if unable to log security audits.
Interactive logon: Do not display last user name	Do not display last user name in the Log On to Windows dialog box
Interactive logon: Do not require CONTROL+ALT+DEL	Do not require CONTROL+ALT+DEL to logon
Interactive logon: Message text for users attempting to logon	Message text for users attempting to logon
Interactive logon: Message title for users attempting to logon	Message title for users attempting to logon
Interactive logon: Number of previous logons to cache	Number of previous logons to cache (in case domain controller is not available)
Interactive logon: Prompt user to change password before expiration	Prompt user to change password before expiration (days)
Screen Saver: Inactivity period	The number of seconds the system must remain idle before the screen saver starts. [HKCU]
Screen Saver: Password protected	Indicates whether the screen saver is password-protected. [HKCU]
Screen Saver: Screen Savers run	Indicates whether or not a screen saver is selected. [HKCU]
Shutdown: Allow system to be shut down without having to log on	Allow system to be shut down without having to log on
Shutdown: Clear virtual memory pagefile	Clear virtual memory pagefile

Services Properties

Checkpoint	A value that the service increments periodically to report its progress during a lengthy start, stop, pause, or continue operation.
Controls Accepted	The control codes that the service will accept and process in its handler function.
Display Name	The friendly name of the service displayed by user interface programs.
Error Control	The severity of the error if this service fails to start during startup, and determines the action taken by the startup program if failure occurs.
Load Order Group	The load ordering group of which this service is a member.
Logon Name	The account name that the service process will be logged on as when it runs.
Path Name	The path to the service binary file.
Service Name	A service in a service control manager database.
Service Specific Exit Code	A service-specific error code that the service returns when an error occurs while the service is starting or stopping.
Service Type	The type of service. E.g. Kernel Driver, Own Process.
Start Type	When to start the service. E.g. Automatic, Boot, Manual.
State	The current state of the service. E.g. Stopped, Running.
Tag Id	A unique tag value for this service in the Load_Oder_Group group.
Wait Hint	An estimate of the amount of time, in milliseconds, that the service expects a

	pending start, stop, pause, or continue operation to take before the service makes its next call to the system.
Win32 Exit Code	An error code that the service uses to report an error that occurs when it is starting or stopping.

Dependent Service Properties

Dependent Service	The Main_Service is dependent on this service.
Dependent Service Type	Type of 'Dependency' service
Depending Service	This service is dependent on the 'Dependency' service

Shares Properties

Current Uses	The number of current connections to the resource
Description	An optional comment regarding the shared resource
Max Uses	The maximum number of concurrent connections that the shared resource can accommodate. -1 = unlimited.
Path	The local path for the shared resource
Permissions	The shared resource's permissions for servers running with share-level security. A server running user-level security ignores this member.
Share Name	The share name of a resource
Share Type	The type of the shared resource. E.g. File Share, Print Queue

User Account Properties

Account Disabled?	Has the account been disabled?
Account Expiry Date	The time the account is set to expire. (UTC time).
Account Functional?	A composite value that indicates whether the account can be used to login to the system. No = the account is either Expired, Disabled or Locked.
Account Locked?	Is the account locked due to invalid signon attempts?
Account Name	The name of the account
Account not Delegated	Marks the account as "sensitive"; other users cannot act as delegates of this user account. (not supported for Win NT)
Bad Password Count (NR)	The number of times the user tried to log on to the account using an incorrect password (not replicated across DCs)
Code Page	The code page for the user's language of choice
Comment	A remark associated with the user account (usri3_comment)
Country Code	The country/region code for the user's language of choice
DC Account?	A computer account for a backup domain controller that is a member of this domain
Domain Trust Account?	A permit to trust account for a domain that trusts other domains
Full Name	User's full name

Group Memberships	The number of security groups that the account is a member of
Home Directory	The user's Home directory
Home Directory Drive	The drive letter assigned to the user's home directory for logon purposes
Last Logon Date	The time that the account last logged into the system (UTC time).
Local Account?	An account for users whose primary account is in another domain.
Logon Hours	A 21-byte (168 bits) bit string that specifies the times during which the user can log on. Each bit represents a unique hour in the week, in Greenwich Mean Time (GMT).
Logon Server	The name of the server to which logon requests are sent. * indicates that logon requests can be handled by any logon server.
Max Disk Space Allowed	The maximum amount of disk space the user can use. -1 = unlimited.
No Auth Data Required	Indicates that when the key distribution center (KDC) is issuing a service ticket for this account, the privilege attribute certificate (PAC) MUST NOT be included. See [RFC4120] for more information.
No Preauthentication	The account does not require Kerberos preauthentication for logon. (not supported for Win NT)
Normal Account?	A default account type that represents a typical user
Number of Logons (NR)	The number of times the user logged on successfully to this account (not replicated across DCs)
Password Change Date	The time that the account's password was last changed (local time on the Scan Client).
Password Expired	The user's password has expired. (not supported for Win NT / 2000)
Password Expired?	Has the password expired?
Password Never Expires?	Does the password never expire?
Password Not Required?	Can the account login without a password?
Primary Group Id (PID)	The RID of the Primary Global Group for the user
Privilege	The privilege assigned to the account (Administrator, User or Guest). Not relevant for domain accounts on systems with Active Directory.
Profile Path	The path to the user's profile
Read Only DC	Indicates that the account is a computer account for a read-only domain controller (RODC). Only interpreted by a DC whose DC functional level is DS_BEHAVIOR_WIN2008 or greater.
Reversible Password Encryption	The user's password is stored under reversible encryption in the Active Directory (not supported for Win NT)
Script Executed?	The logon script executed (always set)
Script Path	The path for the user's logon script file
Smart Card Required	Requires the user to log on to the user account with a smart card (not supported for Win NT)
Trusted for Delegation	The account is enabled for delegation. Allows a service running under the account to assume a client's identity and authenticate as that user to other remote servers. (not supported for Win NT)
Trusted to Authenticate for Delegation	The account is trusted to authenticate a user outside of the Kerberos security package and delegate that user through constrained delegation. (not supported for Win NT / 2000 / XP)

Units per Week (for Logon Hours)	The number of equal-length time units into which the week is divided. This value is required to compute the length of the bit string in the Logon_Hours field.
Use DES Encryption	Restrict this account to use only DES encryption types for keys. (not supported for Win NT)
User Cannot Change Password?	Is the user prevented from changing the password?
User Comment Text	A remark associated with the user account (usri3_usr_comment)
User Id (UID)	The relative ID (RID) of the user
Workstation Account?	A computer account for a computer that is a member of this domain
Workstations Allowed	The names of workstations from which the user can log on (if blank the user can logon from any workstation)