

---

# Product Specification

## SekChek Local: Active Directory

---

---

First Published: August, 2008  
Last Revision: August, 2010

Copyright © 2008-2010, SekChek IPS  
Tel: +27 (11) 461 7900  
[inbox@sekchek.com](mailto:inbox@sekchek.com)  
[www.sekchek.com](http://www.sekchek.com)



## Contents

---

<b>1. Main Features</b>	<b>4</b>
<b>2. Summary of Reports &amp; Analyses</b>	<b>7</b>
<i>Effective Domain Account Policies</i>	7
<i>Group Policy Objects</i>	7
<i>GPO Policies</i>	8
<i>MS-Exchange Objects</i>	8
<i>User Accounts</i>	8
<i>Group Accounts</i>	9
<i>Directory Server (DS) System Configuration</i>	9
<i>Other Reports</i>	10
<b>3. Detailed List of Attributes Analysed</b>	<b>11</b>
<i>Base Board Properties</i>	11
<i>BIOS Properties</i>	11
<i>Computer Properties</i>	11
<i>Disk Properties</i>	12
<i>Domain Controller Properties</i>	12
<i>Domain Properties</i>	13
<i>Exchange Databases [from V1.4.5]</i>	15
<i>Exchange Organisation [from V1.4.5]</i>	15
<i>Exchange Servers [from V1.4.5]</i>	16
<i>Exchange Storage Groups [from V1.4.5]</i>	18
<i>Exchange Users [from V1.4.5]</i>	18
<i>FSMO Role Owner Properties</i>	19
<i>GPO Container Properties</i>	20
<i>GPO Link Properties</i>	20
<i>GPO Policies</i>	20
<i>Group Member Properties</i>	22
<i>Group Properties</i>	22
<i>Host Roles</i>	23
<i>Hot Fixes Installed on the System</i>	24
<i>Network Adapters</i>	24
<i>Operating System Properties</i>	25
<i>OS Recovery Options [from V1.4.2]</i>	26
<i>OU Properties</i>	27
<i>Page File Properties</i>	27
<i>Permissions Properties</i>	27
<i>Processor Properties</i>	28
<i>Products Installed [from V1.4.5]</i>	29
<i>Password Setting Objects (PSOs) [from V1.4.4]</i>	29
<i>Services Properties [from V1.4.0]</i>	30



# Product Specification: SekChek Local (AD)

Version 1.4.5

---

<i>Shares Properties [from V1.4.4]</i>	31
<i>Dependent Service Properties [from V1.4.0]</i>	31
<i>Site Properties</i>	31
<i>Trusted Domain Properties</i>	31
<i>User Account Properties</i>	32



## 1. Main Features

The **Local AD tool** analyses *domain-wide* security policies and security objects defined in a single Active Directory domain. I.e. the target is an Active Directory domain, rather than a specific Server or computer.

SekChek scans most security objects and control settings defined in the target domain, including User & Group accounts, Trusted Domains, OUs, Sites, Account policies, GPOs, PSOs, Services, Network Shares and system configuration data.

### The Local Active Directory (AD) Tool...



- Analyses security on any Windows Active Directory Domain from a single point on the network
- 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 scan security of an entire Active Directory domain from 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.

The screenshot displays the SekChek application window with several key components:

- Navigation Pane:** Located on the left, it contains a 'Summary Bar Chart: User Accounts' and a 'Summary Report: User Accounts'.
- Main Report Area:**
  - Graphical Summary:** A bar chart titled 'User Accounts Summary: World C' showing percentages for Administrator Privilege (12.0%), Functional Accounts (16.0%), Non-Functional Accounts (16.0%), and Disabled (9.3%).
  - Summary Report:** A table titled 'Summary of User Accounts: World Communica' with columns for 'Number' and 'Percent'. It lists categories like Total User Accounts (75, 100.00%), Administrator Privilege (9, 12.00%), Non-administrative Accounts (66, 88.00%), User Accounts: Functional (63, 84.00%), User Accounts: Non-Functional (12, 16.00%), and User Accounts: Expired (1, 1.33%).
  - Standard Reports:** A 'List Users: Password Last Changed (> Days)' table with columns for 'CN' and 'Password Change Date'. It lists users such as Achmed Hussain, Adam Burke, Administrator, Adri Palmer, Aileen Hayden, Albert Eksteen, Ali Khan, Andre Greyvensteyn, Andrea Teague, Ashley Naidoo, Barry Bailey, and Brardl Ratson.
  - Detailed Report:** A 'SekChek Report (AD) Menu: V1.4.4 (24-Apr-2010)' window showing report parameters, scan details, and a 'Go To' field.
- Toolbar:** At the top, it includes 'Sort & Filter' and 'Search' buttons, which are highlighted with purple arrows.



## Product Specification: SekChek Local (AD)

Version 1.4.5

---

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.



## 2. Summary of Reports & Analyses

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

- Which Users have not changed their password in the last 90 days?
- Does the Domain policy comply with your standards for password change frequency and minimum password length?
- What is the percentage of accounts with Administrator privileges?
- Which User accounts have not been used in the last 60 days, so may be redundant?
- Which Group accounts were defined in the last 30 days?

Familiar selection boxes allow you to select a Report and quickly scroll through a series of detailed reports or high-level summary views.

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

### **Effective Domain Account Policies**

Report Description	Detailed	Summary
Administrator Account Status (Renamed / Disabled)	X	X
Guest Account Status (Renamed / Disabled)	X	X
Lockout Duration / Threshold / Observation Window	X	X
Maximum / Minimum Password Age	X	X
Minimum Password Length	X	X
Native Mode	X	X
Password History Length	X	X

### **Group Policy Objects**

Report Description	Detailed	Summary
GPO Containers, Properties & Status	X	X
GPO Links to Organisational Units	X	X
GPO Policies	X	
GPOs not Found in Active Directory	X	X
GPOs not Found on Disk	X	X



### ***GPO Policies***

<b>Report Description</b>	<b>Detailed</b>	<b>Summary</b>
Password Policy	X	X
Account Lockout Policy	X	X
Kerberos Policy	X	X
Audit Policy	X	X
Event Log Policy	X	X

### ***MS-Exchange Objects***

<b>Report Description</b>	<b>Detailed</b>	<b>Summary</b>
Databases	X	
Organisation	X	
Servers	X	
Storage Groups	X	
Users	X	

### ***User Accounts***

<b>Report Description</b>	<b>Detailed</b>	<b>Summary</b>
Accounts Changed in the Last 30 / 60 / 90 / 180 / 360 Days	X	X
Accounts Created in the Last 30 / 60 / 90 / 180 / 360 Days	X	X
Administrative Accounts	X	X
All User Accounts	X	X
Cannot Change Password	X	X
Functional Accounts	X	X
Last Logon > 30 / 60 / 90 / 180 / 360 Days	X	X
Last Logon Never	X	X
Logon Hours Restricted	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



Report Description	Detailed	Summary
Password Last Changed Never	X	X
Password Never Expires	X	X
Password Not Required	X	X
Password Stored with Reversible Encryption	X	X
Remote Dial-In Allowed	X	X
Smart Card Required	X	X

### **Group Accounts**

Report Description	Detailed	Summary
All Security Groups	X	X
Global Groups	X	X
Groups Changed in the Last 30 / 60 / 90 / 180 / 360 Days	X	X
Groups Created in the Last 30 / 60 / 90 / 180 / 360 Days	X	X
Group Members	X	
Groups that Grant Administrative Privileges	X	X
Groups with no Members	X	X
Local Groups	X	X
Universal Groups	X	X

### **Directory Server (DS) System Configuration**

Report Description	Detailed	Summary
Base Board	X	X
BIOS	X	X
Computer Config	X	X
Disk Drives	X	X
Hot Fixes, SPs	X	X
Host Roles	X	X
Network Adapters	X	X
Network Shares [from V1.4.4]	X	X
Operating System	X	X



Report Description	Detailed	Summary
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
Directory Auditing (SACLs)	X	
Directory Permissions (DAACLs)	X	
Domain Controllers	X	X
FSMO Role Owners	X	X
Organisational Units	X	X
Password Setting Objects [from V1.4.4]	X	X
Services [from V1.4.0]	X	X
Sites	X	X
Trusted Domains	X	X



### 3. Detailed List of Attributes Analysed

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

#### **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.

## Domain Controller Properties

Common Name	The Common Name of the Domain Controller (DC)
Description	A freeform description
Disable Inbound Replication	Indicates whether inbound replication is disabled for this DC
Disable Outbound Replication	Indicates whether outbound replication is disabled for this DC
DNS Name	The DNS name of the DC. E.g. 'MyServer.IPS.SekChek.com'
Global Catalog Server	Indicates whether this is a Global Catalog Server



# Product Specification: SekChek Local (AD)

## Version 1.4.5

GUID	Globally Unique Identifier for the account. E.g. 21EC2020-3AEA-1069-A2DD-08002B30309D [from V1.4.5]
IP Address	The IP address of the Domain Controller [from V1.4.4]
Operating System	The OS installed on the Domain Controller. E.g. Windows Server 2003
OS Service Pack	The Service Pack installed on the system. E.g. Service Pack 2
OS Version	The version of the Operating System. E.g. 5.2 (3790)
Path Id	The DC's Path Id
Primary Group Id (PID)	The RID of the Primary Global Group for the DC
SAM Account Name	The SAM name for the DC (must be < 20 characters to support clients prior to Win2000)
Scanned For LastLogons	Indicates whether the DC was scanned for Users' Last Logon details
SID	Security Identifier (SID) for the Domain Controller
When Changed	When the DC object was last changed (UTC). Not replicated across DCs.
When Created	When the DC object was created (UTC). This value is replicated and is in the global catalog.

### Domain 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
Block Policy Inheritance	Blocks GPOs that apply higher in the Active Directory hierarchy of sites, domains, and OUs. It does not block GPOs if they have No Override enabled. Set on the Domain or OU, not on the GPO.
Client Machine	The machine from which the Scan was run. E.g. CN=MyPC,CN=Computers,DC=IPS,DC=SekChek,DC=com
Configuration Container	Distinguished name for the configuration container
DC Functionality Level	The functional level of the Domain Controller (from Win 2003) [from V1.4.4]
Directory Server	DNS address for the Directory Server queried by the Scan
Domain Functionality Level	The functional level of the Domain (from Win 2003) [from V1.4.4]
Domain Name (DNS)	The DNS name of the target domain. E.g. 'IPS.SekChek.com'
Domain Name (LDAP)	The LDAP name (DN) of the target domain. E.g. 'DC=IPS,DC=SekChek,DC=com'
Domain name (short)	The short name of the target domain. E.g. 'IPS'
Force Logoff	Indicates whether users are forced off the system when their valid logon hours expire. -1: never forced to log off. 0: forced to log off immediately when the valid logon hours expire.
Forest DNS Name	The DNS name of the Domain's forest
Forest Functionality Level	The functional level of the Forest (from Win 2003) [from V1.4.4]



# Product Specification: SekChek Local (AD)

## Version 1.4.5

GUID	Globally Unique Identifier for the domain. E.g. 21EC2020-3AEA-1069-A2DD-08002B30309D [from V1.4.5]
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
Native Mode	Indicates whether the domain is in native or mixed mode
OS Build Nbr	The build number of the OS on the Directory Server
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)
Protected From Accidental Deletion	Indicates whether the 'Protect object from accidental deletion' flag is enabled for the object. (from Win 2008) [from V1.4.5]
Reversible Passwords	The user's password is stored under reversible encryption in the Active Directory (Windows 2000/XP)
Scan Account	The account used to perform the Scan. E.g. CN=Administrator,CN=Users,DC=IPS,DC=SekChek,DC=com
Scan Time	The time that the Domain was Scanned (Local time on the client system)
Schema Container	Distinguished name for the schema container
Server DN	Distinguished name for the Server queried by the Scan
Server OS	The Directory Server's Operating System
Service Pack	The Window's Service Pack installed on the Directory Server
SID: Domain	Security Identifier (SID) for the domain.
Site Name	The name of the DC's Site
Supported SASL Mechanisms	Security mechanisms supported for SASL negotiation. By default, GSSAPI is supported.
Time Zone Bias	The time zone bias, relative to GMT, on the machine where the Scan was run
When Changed	When the Domain object was last changed (UTC). Not replicated across DCs.
When Created	When the Domain object was created (UTC). This value is replicated and is in the global catalog.



## ***Exchange Databases [from V1.4.5]***

Age Limit For SubFolders in Database (Days)	Age limit for all folders in this public folder database (Public Folders only)
Database	The name of the database
Database Can Be Overwritten By A Restore	This database can be overwritten during a restore process.
Database Path	Database path
Database Type	Mailbox or Public Folder
Delete Event Log Entries Older Than (Days)	Delete event log entries older than days
Delete Items After Database Backup	Do not permanently delete items until database has been backed up
Exchange Server	The Exchange Server that owns the Storage group
GUID	Globally Unique Identifier for the object.
Issue Warning At (KB)	Issue warning at (KB)
Journal Recipient	Journal recipient
Journal Recipient Path Id	Journal recipient pathId
Keep Deleted Items For (days)	Keep deleted items for days
Keep Deleted Mailboxes For (Days)	Keep deleted mailboxes for days (Mailboxes only)
Maximum Item Size (KB)	Maximum item size KB (Public Folders only)
Offline	Indicates whether the database is offline.
Prohibit Send And Receive/Post At (KB)	Prohibit send and receive/post at KB
Prohibit Send At (KB)	Prohibit send at KB (Mailboxes only)
Replication Interval For "Always Run" (Minutes)	Replication interval for "Always Run" (minutes)
Replication Message Size Limit (KB)	Replication message size limit (KB)
Replication Scheduled	Replication scheduled
Storage Group	The Exchange Storage group
When Changed	When the object was last changed (UTC). Not replicated across DCs.
When Created	When the object was created (UTC). This value is replicated and is in the global catalog.

## ***Exchange Organisation [from V1.4.5]***

Description	A freeform description
Exchange Organisation	The Exchange organisation name
GUID	Globally Unique Identifier for the object.
Organisation Mixed Mode	Exchange organisation mode
Version Number	The version number for the object



# Product Specification: SekChek Local (AD)

## Version 1.4.5

When Changed	When the object was last changed (UTC). Not replicated across DCs.
When Created	When the object was created (UTC). This value is replicated and is in the global catalog.

### **Exchange Servers [from V1.4.5]**

CN	The Exchange server's Common Name
Admin Group	The Exchange Administrative group
Client Access Role	Client Access role (CAS). (from Exchange 2007)
Connectivity Logging Enabled	Specifies whether Connectivity logging is enabled
Default Storage Group Path	The default storage group path
Edge Transport Role	Edge Transport role. (from Exchange 2007)
ELC Log File Size Limit	Email Life Cycle (ELC) log file size limit
ELC Log Path	Email Life Cycle (ELC) log file path
Enable Message Tracking Logging	Indicates whether Message Tracking logging is enabled on the server
Enable Subject Logging & Display	Enable subject logging and display (Exchange 2003 only)
Exchange Version	Exchange version. E.g. Version 8.2 (Build 30176.2)
External DNS Servers	List of manually-entered DNS servers used by Send connectors that are configured to use the external DNS lookup configuration on the transport server.
GUID	Globally Unique Identifier for the object
Hub Transport Role	Hub Transport role. (from Exchange 2007)
Installation Path	The installation path for Exchange
Internal DNS Servers	List of manually-entered DNS servers used by connectors that resolve IP addresses for servers inside the organization
Mailbox Role	Mailbox role. (from Exchange 2007)
Max Concurrent Outbound Connections	Maximum concurrent outbound connections
Max Concurrent Outbound Connections (per Domain)	Maximum concurrent outbound connections per domain
Max Time Since Submission (Days)	Maximum time since submission (days)
Maximum Connectivity Logfile Age (Days)	Maximum connectivity log file age (days)
Maximum Message Tracking Log Directory Size	The maximum size of the directory for the Message Tracking log
Maximum Message Tracking Logfile Age (Days)	Maximum Message Tracking log file age (days)
Maximum Message Tracking Logfile Size	The maximum size of the log file for the Message Tracking log
Maximum Pickup Directory Header Size	Maximum Pickup directory header size
Maximum Pickup Directory Message Per Minute	Maximum Pickup directory messages per minute
Maximum Pickup Directory Recipients	Maximum Pickup directory recipients
Maximum Receive Connector protocol Log File Age (Days)	Maximum Receive connector protocol log file age (days)



# Product Specification: SekChek Local (AD)

## Version 1.4.5

Maximum Routing Log Directory Size	Maximum Routing log directory Size
Maximum Routing Log File Age (Days)	Maximum Routing log file age (days)
Maximum Send Connector protocol Log File Age (Days)	Maximum Send Connector protocol log file age (days)
Message Poisons Threshold	Messages with this number of poisons or more are moved to the poison message queue
Message Retry Interval	Specifies the retry interval for individual messages that have a status of Retry.
Message Tracking Log File Path	Message Tracking log file path
msExchEdgeSyncAdamLdapPort	The LDAP port to which the Microsoft Exchange EdgeSync service binds when synchronizing data from Active Directory to ADAM. By default, this is TCP port 50389.
Notify Sender After Delay Hours	Notify sender when message is delayed more than (hours)
Outbound Connection Failure Retry Interval (Mins)	Outbound connection failure retry interval (minutes)
Pickup Directory Path	Pickup directory path
Product Id	Exchange product Id. (from Exchange 2007)
Receive Connector Protocol Log File Path	Receive connector protocol log file path
Receive Connector Protocol Log: Max Directory Size	The maximum size of the directory for the Receive Protocol log
Receive Connector Protocol Log: Max File Size	The maximum size of the log file for the Receive Protocol log
Remove Log Files Older Than (Days)	Remove log files older than (days). (Exchange 2003 only)
Replay Directory Path	Replay directory path
Routing Log File Path	Routing log file path
Secure LDAP Port	The secure LDAP port to which the Microsoft Exchange EdgeSync service binds when synchronizing data from Active Directory to ADAM. By default, this is TCP port 50636.
Send Connector Protocol Log File Path	Send connector protocol log file path
Send Connector Protocol Log: Max Directory Size	The maximum size of the directory for the Send Protocol log
Send Connector Protocol Log: Max File Size	The maximum size of the log file for the Send Protocol log
Transient Failure Retry Attempts	Transient failure retry attempts
Transient Failure Retry Interval (seconds)	Transient failure retry interval (seconds)
Transport Connectivity Log: Max Directory Size	The maximum size of the directory for the Transport Connectivity log
Transport Connectivity Log: Max File Size	The maximum size of the log file for the Transport Connectivity log
Transport Connectivity: Log Path	Transport connectivity log file path
Unified Messaging Role	Unified Messaging role. (from Exchange 2007)
Use Manually Configured External DNS Servers	Specify whether to use the External Domain Name System (DNS) servers that are associated with a network adapter or manually entered DNS servers.
Use Manually Configured Internal DNS Servers	Specify whether to use the Internal Domain Name System (DNS) servers that are associated with a network adapter or manually



	entered DNS servers.
When Changed	When the object was last changed (UTC). Not replicated across DCs.
When Created	When the object was created (UTC). This value is replicated and is in the global catalog

### ***Exchange Storage Groups [from V1.4.5]***

Enable Circular Logging	Indicates whether circular logging is enabled
Exchange Server	The Exchange Server that owns the Storage group
GUID	Globally Unique Identifier for the object.
Log File Prefix	Log file prefix. E.g. E01
Log Path	Log path
Storage Group	Storage Group Name
System Path	System path
When Changed	When the object was last changed (UTC). Not replicated across DCs.
When Created	When the object was created (UTC). This value is replicated and is in the global catalog.

### ***Exchange Users [from V1.4.5]***

CN	The Common Name for the account
Accept Messages From All Senders	Accept Messages from all senders
Deleted Item Retention: Use Mailbox Database Defaults	Deleted item retention: Use mailbox database defaults
Deliver and Redirect	Deliver message to both forwarding address and mailbox
Display Name	The name of the object as it appears in the Global Address List
Enable Retention Hold	Enable retention hold for items in this mailbox
extensionAttribute1	An attribute for any text without having to extend Active Directory
extensionAttribute10	An attribute for any text without having to extend Active Directory
extensionAttribute11	An attribute for any text without having to extend Active Directory
extensionAttribute12	An attribute for any text without having to extend Active Directory
extensionAttribute13	An attribute for any text without having to extend Active Directory
extensionAttribute14	An attribute for any text without having to extend Active Directory
extensionAttribute15	An attribute for any text without having to extend Active Directory
extensionAttribute2	An attribute for any text without having to extend Active Directory
extensionAttribute3	An attribute for any text without having to extend Active Directory
extensionAttribute4	An attribute for any text without having to extend Active Directory
extensionAttribute5	An attribute for any text without having to extend Active Directory



extensionAttribute6	An attribute for any text without having to extend Active Directory
extensionAttribute7	An attribute for any text without having to extend Active Directory
extensionAttribute8	An attribute for any text without having to extend Active Directory
extensionAttribute9	An attribute for any text without having to extend Active Directory
Forward To	An alternative recipient to receive e-mail
Forward to Path Id	Forward to recipient path Id
Hide From Exchange Address Lists	Hide from Exchange address lists
Issue Warning After (KB)	Issue warning when the mailbox reaches this size (KB)
Keep Deleted Items For (days)	Keep deleted items for (days). Default = 14 days.
Mail Alias	The user's mail alias (mail Nickname)
Mailbox Database	The user's mailbox database. E.g. Second Mailbox Database
Mailbox Server	The mailbox Server
Mailbox Storage Group	The mailbox storage group. E.g. Second Storage Group
Max Receive Size (KB)	Amount of data, in kilobytes (KB), that you are allowed to receive
Max Send Size (KB)	The maximum length, in kilobytes (KB), of a message that can be sent
Maximum Recipients	Maximum recipients
Path Id	The user's Path Id
Primary SMTP Address	The user's primary SMTP email address
Prohibit Send & Receive After (KB)	Prohibit sending & receiving email when the mailbox reaches this size (KB)
Prohibit Send After (KB)	Prohibit sending email when the mailbox reaches this size (KB)
Reject Messages From No Senders	Reject messages from no senders
Require Sender Authentication	Require that all senders are authenticated
Retention Hold End Date	Enable retention hold for items in this mailbox (End date)
Retention Hold Start Date	Enable retention hold for items in this mailbox (Start date)
Storage Quotas: Use MailBox Database Defaults	Storage quotas: Use mailbox database defaults

### **FSMO Role Owner Properties**

Domain Naming Master	The Domain Naming Master (unique in the enterprise). The only DC that can: Add or remove domains to the forest; Add or remove cross-reference objects to external directories.
Infrastructure Master	The Infrastructure Master (unique per domain). Updates the cross-domain group-to-user reference to reflect the user's new name.
PDC Emulator	The PDC Emulator (unique per domain). Receives preferential replication of password changes performed by other DCs in the domain and handles password authentication requests that fail at the local DC.
RID Master	The RID Master (unique per domain). Allocate sequences of relative IDs to each domain controller in its domain.



Schema Master	The Schema Master (unique in the enterprise). The only domain controller that can perform write operations to the directory schema.
---------------	---

### **GPO Container Properties**

CN	The GPO Container's Common Name
Computer Config Disabled	Indicates whether the GPO's Computer Configuration settings are disabled
Display Name	The display name for the Group Policy Object (GPO)
GPO Exists on Disk	Indicates whether the GPO exists on disk. No = file GptTmpl.inf was not found in the SYSVOL path.
GPO Functionality Version	The version of the Group Policy Editor that created the GPO
GPO Location on Disk	The location of the GPO on the Directory Server's file system
GPO Policies	The policies defined in the GPO
Path Id	The Container's Path Id
User Config Disabled	Indicates whether the GPO's User Configuration settings are disabled
When Changed	When the GPO Container was last changed (UTC). Not replicated across DCs.
When Created	When the GPO Container was created (UTC). This value is replicated and is in the global catalog.

### **GPO Link Properties**

Domain / Site / OU	The name of the Domain, Site or OU with the link to the GPO
GPO Disabled	Ensures that the settings in the GPO no longer apply to users or computers in the site, domain, or OU to which the GPO was linked. This includes objects in child Containers.
GPO PathId	The Path Id for the linked GPO
GPO Priority	The priority of the GPO (1 = high). GPOs with a higher priority have higher precedence because, by default, they can overwrite the objects that are processed earlier.
Linked GPO	The GPO that is linked to the Domain, Site or OU
No Override	Enforces policy inheritance. Forces all child policy containers to inherit the parent's policy, even if that policy conflicts with the child's policy and even if Block Inheritance has been set for the child.
Object Type	The type of the object with the GPO link. E.g. Domain, Site, OU
Path Id	The object's Path Id

### **GPO Policies**

CN	The GPO Container's Common Name
Path Id	The Container's Path Id
Minimum Password Age	The minimum number of days allowed between password changes



# Product Specification: SekChek Local (AD)

## Version 1.4.5

Maximum Password Age	The maximum number of days allowed between password changes
Minimum Password Length	The minimum allowed password length
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 Size	The number of previous passwords remembered by Windows (prevents passwords from being cycled)
Account Lockout Threshold	The number of invalid password authentications that can occur before an account is 'locked'.
Reset Account Lockout After	The maximum time, in minutes, that can elapse between the number of failed logon attempts defined in 'Lockout Threshold' before lockout occurs.
Account Lockout Duration	The time in minutes that a locked account remains locked before it is automatically unlocked.
Store Passwords Reversible Encryption	The user's password is stored under reversible encryption in the Active Directory (Windows 2000/XP)
Force Logoff when Logon Hours Expire	Indicates whether users are forced off the system when their valid logon hours expire.
Rename Guest Account	Indicates whether the GPO enforces renaming of the Guest account.
Audit System Events	Audit attempts to shut down or restart the computer. Also, audit events that affect system security or the security log.
Audit Logon Events	Audit attempts to log on to or log off from the system. Also, audit attempts to make a network connection.
Audit Object Access	Audit attempts to access securable objects, such as files.
Audit Privilege Use	Audit attempts to use Windows privileges.
Audit Policy Change	Audit attempts to change Policy object rules.
Audit Account Management	Audit attempts to create, delete, or change user or group accounts. Also, audit password changes.
Audit Process Tracking	Audit events such as program activation, some forms of handle duplication, indirect access to an object, and process exit.
Audit DS Access	Audit attempts to access the directory service.
Audit 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.
Max Lifetime for User Ticket	Determines the maximum amount of time (in hours) that a user's ticket-granting ticket (TGT) may be used.
Max Lifetime for User Ticket Renewal	This security setting determines the period of time (in days) during which a user's ticket-granting ticket (TGT) may be renewed.
Max Lifetime for Service Ticket	Determines the maximum amount of time (in minutes) that a granted session ticket can be used to access a particular service.
Max Tolerance for Clock Synch	Determines the maximum time difference (in minutes) that Kerberos V5 tolerates between the time on the client clock and the time on the DC running Windows 2003 that provides Kerberos authentication.
Enforce User Logon Restrictions	Determines whether the Kerberos V5 Key Distribution Center (KDC) validates every request for a session ticket against the user rights policy of the user account.



# Product Specification: SekChek Local (AD)

## Version 1.4.5

Maximum application log size	Maximum application log size (KB)
Maximum security log size	Maximum security log size (KB)
Maximum system log size	Maximum system log size (KB)
Prevent local guests group from accessing application log	Prevent local guests group from accessing application log
Prevent local guests group from accessing security log	Prevent local guests group from accessing security log
Prevent local guests group from accessing system log	Prevent local guests group from accessing system log
Retain application log	Retention period for the application log.
Retain security log	Retention period for the security log.
Retain system log	Retention period for the system log.
Retention method for application log	Retention method for the application log. E.g. By days, As needed
Retention method for security log	Retention method for the security log. E.g. By days, As needed
Retention method for system log	Retention method for the system log. E.g. By days, As needed

### Group Member Properties

Group CN	The Group's Common Name
Group PathId	The Group's Path Id
Member Class	The member's Object Class. E.g. computer; foreignSecurityPrincipal; Group; User
Member CN	The Group Member's Common Name
Member Domain	The Group Member's domain (if different to the scanned domain)
Member PathId	The Group Member's Path Id
Member SAM Account	The account name assigned by the Security Accounts Manager. (must be < 20 characters to support clients prior to Win2000)
Member SID	Security Identifier (SID) for the member

### Group Properties

Administrator Privilege	Indicates whether the group has Administrator privilege. The privilege is gained via direct or indirect membership of the Administrators group.
CN	The Group's Common Name
Description	A remark associated with the group
Group Id	The relative identifier of the global group
Group Type	The type of Group. E.g. Global, Local, Universal
GUID	Globally Unique Identifier for the account. E.g. 21EC2020-3AEA-1069-A2DD-08002B30309D [from V1.4.5]
Path Id	The Group's Path Id
Protected From Accidental	Indicates whether the 'Protect object from accidental deletion' flag is enabled for the



# Product Specification: SekChek Local (AD)

## Version 1.4.5

Deletion	object. (from Win 2008) [from V1.4.5]
Redundant?	If 'Yes', the group does not contain any members
SAM Account Name	The account name assigned by the Security Accounts Manager. (must be < 20 characters to support clients prior to Win2000)
SID	The unique security identifier for the group
When Changed	When the group account was last changed (UTC). Not replicated across DCs.
When Created	When the account was created (UTC). This value is replicated and is in the global catalog.

### 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



# Product Specification: SekChek Local (AD)

## Version 1.4.5

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 or 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 apps)	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]



# Product Specification: SekChek Local (AD)

## Version 1.4.5

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.



### OU Properties

Block Policy Inheritance	Blocks GPOs that apply higher in the Active Directory hierarchy of sites, domains, and OUs. It does not block GPOs if they have No Override enabled. Set on the Domain or OU, not on the GPO.
Description	A freeform description of the OU
GUID	Globally Unique Identifier for the object. E.g. 21EC2020-3AEA-1069-A2DD-08002B30309D [from V1.4.5]
Organisational Unit	The name of the Organisational Unit
Path Id	The OU's Path Id
Protected From Accidental Deletion	Indicates whether the 'Protect object from accidental deletion' flag is enabled for the object. (from Win 2008) [from V1.4.5]
When Changed	When the OU was last changed (UTC). Not replicated across DCs.
When Created	When the OU was created (UTC). This value is replicated and is in the global catalog.

### 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,



# Product Specification: SekChek Local (AD)

## Version 1.4.5

	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



# Product Specification: SekChek Local (AD)

## Version 1.4.5

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
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
Name	Label by which the object is known
Nbr	Unique Processor Id
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

### **Password Setting Objects (PSOs) [from V1.4.4]**

PSO CN	The PSO's Common Name
Lockout Duration	The time that a locked account remains locked before it is automatically unlocked. Expressed as DD:HH:MM:SS
Lockout Observation Window	The maximum time that can elapse between the number of failed logon attempts defined in 'Lockout Threshold' before lockout occurs. Expressed as DD:HH:MM:SS
Lockout Threshold	The number of invalid password authentications that can occur before an account is 'locked'.



# Product Specification: SekChek Local (AD)

## Version 1.4.5

Max Password Age	The maximum time allowed between password changes. Expressed as DD:HH:MM:SS
Min Password Age	The minimum time allowed between password changes. Expressed as DD:HH:MM:SS
Min Password Length	The minimum allowed password length
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)
Path Id	The PSO's Path Id
PSO Applies To	The objects that the PSO applies to.
PSO Description	An optional comment regarding the PSO
PSO Display Name	The display name for the PSO
PSO Precedence	The precedence of the Password Settings Object (PSO)
Reversible Passwords	The user's password is stored under reversible encryption in the Active Directory
When Changed	When the PSO was last changed (UTC). Not replicated across DCs.
When Created	When the PSO was created (UTC). This value is replicated and is in the global catalog.

### Services Properties [from V1.4.0]

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_Order_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.



## Shares Properties [from V1.4.4]

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

## Dependent Service Properties [from V1.4.0]

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

## Site Properties

Block Policy Inheritance	Blocks GPOs that apply higher in the Active Directory hierarchy of sites, domains, and OUs. It does not block GPOs if they have No Override enabled. Set on the Site, Domain or OU, not on the GPO.
CN	The name of the Site
Description	A freeform description of the Site
GUID	Globally Unique Identifier for the site. E.g. 21EC2020-3AEA-1069-A2DD-08002B30309D [from V1.4.5]
Path Id	The Site's Path Id
Protected From Accidental Deletion	Indicates whether the 'Protect object from accidental deletion' flag is enabled for the object. (from Win 2008) [from V1.4.5]
When Changed	When the Site was last changed (UTC). Not replicated across DCs.
When Created	When the Site was created (UTC). This value is replicated and is in the global catalog.

## Trusted Domain Properties

CN	The object's Common Name
Flat Name	For Windows NT trusted domains, this is the NetBIOS domain name.
GUID	Globally Unique Identifier for the object. E.g. 21EC2020-3AEA-1069-A2DD-08002B30309D [from V1.4.5]
Path Id	Path Id for the CN
SID	The unique security Identifier



Trust Attributes	The attributes of the trust relationship. E.g. Disallow transitivity, Trust valid only for up-level client
Trust Direction	The direction of the trust. E.g. Trusting, Trusted, Two-way
Trust Partner	The name of the domain with which a trust exists.
Trust Type	The type of trust. E.g. Win2000 or later, MIT Kerberos realm
When Changed	When the trust was last changed (UTC). Not replicated across DCs.
When Created	When the trust was created (UTC). This value is replicated and is in the global catalog.

### ***User Account Properties***

Account Disabled?	Has the account been disabled?
Account Expiry Date	The time the account is set to expire
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 not Delegated	Marks the account as "sensitive"; other users cannot act as delegates of this user account. (not supported for Win NT)
Admin Count	Indicates that the account had it's ACL's changed to a more secure value by the system, because it was a member of one of the administrative groups (directly or indirectly)
Administrator Privilege	Indicates whether the account has Administrator privilege. The privilege is gained via direct or indirect membership of the Administrators group.
Administrator sets callback	Indicates whether the Administrator sets call-back options
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)
Callback	Indicates whether the user must use call-back
Callback Number	The user's call-back number. If not set (blank), a Callback number is not defined.
Caller sets callback	Indicates whether the user can set call-back options
Calling Station Nbr	Indicates whether the user is required to dial-in from a specific number. If not set (blank), the Calling Station Id is not verified.
CN	The Common Name for the account
Comment	A remark associated with the user account (usri3_comment)
Dial-in Allowed	Indicates whether the account has remote access permission. Values: Yes, No or Policy (Control access through Remote Access Policy)
Dial-in Service Type	E.g. Callback Framed, Callback Login
Full Name	User's full name
Group Memberships	The number of security groups that the account is a member of
GUID	Globally Unique Identifier for the account. E.g. 21EC2020-3AEA-1069-A2DD-08002B30309D [from V1.4.5]
Home Directory	The user's Home directory



# Product Specification: SekChek Local (AD)

## Version 1.4.5

Home Directory Drive	The drive letter assigned to the user's home directory for logon purposes
Last Failed Logon Date	The time that the account last failed to log into the system. Not replicated across DCs.
Last Logon Date	The time that the account last logged into the system. Not replicated across DCs.
Last Logon DC	The Domain Controller (SAM name) that authenticated the User's last logon to the domain. Only relevant if the option to 'Query all DCs for Users' Last Logon Times' was selected during the Scan.
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).
Nbr DCs Queried for Last Logons	The number of Domain Controllers that were queried for Users' last logon times. Windows does not replicate Users' last logon times across DCs.
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)
Object Class	The class of the object. E.g. user, inetOrgPerson
Password Change Date	The time that the account's password was last changed
Password Expired	The user's password has expired. (not supported for Win NT / 2000)
Password Never Expires?	Does the password never expire?
Password Not Required?	Can the account login without a password?
Path Id	Path Id for the CN
Primary Group Id (PID)	The RID of the Primary Global Group for the user
Profile Path	The path to the user's profile
Protected From Accidental Deletion	Indicates whether the 'Protect object from accidental deletion' flag is enabled for the object. (from Win 2008) [from V1.4.5]
Reversible Password Encryption	The user's password is stored under reversible encryption in the Active Directory (not supported for Win NT)
SAM Account Name	The SAM name for the account (must be < 20 characters to support clients prior to Win2000)
Script Path	The path for the user's logon script file
SID	Security Identifier (SID) for the account. E.g. S-1-5-21-1322135655-2484133651-2918034349-500
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)
UPN	User Principal Name (UPN). E.g. BenoitD@MyOrg.com
Use DES Encryption	Restrict this account to use only DES encryption types for keys. (not supported for



# Product Specification: SekChek Local (AD)

Version 1.4.5

---

	Win NT)
User Cannot Change Password?	Is the user prevented from changing the password?
User Id (UID)	The relative ID (RID) of the user
When Changed	When the account was last changed (UTC). Not replicated across DCs.
When Created	When the account was created (UTC). This value is replicated and is in the global catalog.
Workstations Allowed	The names of workstations from which the user can log on (if blank the user can logon from any workstation)