

A family of security audit and benchmarking tools...



Supports AS/400, UNIX, Microsoft Windows, Active Directory, Novell /]

Visit SekChek Online

- News, latest software releases
- <u>Technical support</u>
- <u>Sample reports</u>

<u>What is the SekChek Service?</u> <u>Benefits of SekChek</u> <u>Clients and Users</u>

- <u>Technical specifications, brochures</u> <u>Where to Contact Us</u>
- <u>Tips for managing your account</u>
- Email: <u>inbox@sekchek.com</u>

About SekChek IPS

SekChek® IPS is a leading provider of computer security review, auditing and benchmarking tools and has served many of the world's largest companies and public institutions in more than 140 countries since 1996. SekChek's clients include security and audit professionals in IT departments, audit firms, internal audit functions, regulatory compliance and corporate governance departments. SekChek's benchmarking features compare security policies and controls against a unique statistics database containing more than 30 million anonymous and real-life security measurements compiled from 80,000 computer systems across all major industry sectors.

What is the SekChek Service?



SekChek is a convenient and automated computer security against *international l world industry averages*, or your organis standards.

SekChek's comprehensive set of reports defaults and *all* user profiles on your syst security weaknesses they also provide yc implications and suggested corrective act

Summary reports, in easy-to-read graph quickly identify problem areas and comp against *leading practices* and *real-world* from 80,000 computers in more than 140

 SekChek is available for a variety of pla
 NetWare 4 and later releases, all versions Directory, all UNIX variants that are Bot

How does it work?

- You use SekChek to scan security on the target system or domain
- We process the security extract files with our *SekChek* processing engines
- We give you the output report in standard Word processor format

It couldn't be simpler!

Benefits

-

The SekChek Service...

Consistent, objective and comprehensive reporting against leading international standards for security *and* the industry average... including suggested actions to correct weaknesses.

Fast and responsive... guaranteed 24 hour turnaround time... however, ✓ same-day service is normally provided.

Convenient and easy-to use... requires no precious time or specialistknowledge from your staff... we do the work for you!

Economical... no software licensing fees... you pay only when you use the service.

No software is installed on the target system... the processing is done offline by our *SekChek* processing engine... no impact on the performance of your system.

Regular users experience significant and lasting improvements in their
 security controls, which typically rank amongst the top 20% in their industry.

If you find this service useful, enquire about the additional benefits and generous discounts available for subscription and volume purchases.

SekChek Local vs SekChek Classic

The following table compares the main features of SekChek's Classic and Local tools. It will help you to decide which tool is right for you.

Features	SekChek Local	SekChek Classic
Caters for all major computer platforms	Supports MS-Windows, Active Directory and MS- Exchange.Support for other platforms is being considered.	Supports MS-Windows, Active Directory, OS/400, UNIX and Novell / Netware and MS- Exchange.
Minimal impact on the target Host	YesThe Scan is executed against the Host system from a workstation attached to the network.	YesAlthough the Scan executes on the target Host it does not use a traditional Setup program and makes no changes to the system.
Analyses multiple systems in one Scan	YesYou can analyse up to 15 Servers per Scan. This makes it easy to compare security across multiple Hosts.	NoThe Scan must be executed on each Host you want to analyse.
Pay as you use service, no software licensing fees, regular software updates	YesYou may copy the software & distribute it in its current form to anyone you wish.	YesYou may copy the software & distribute it in its current form to anyone you wish.
Scan data is processed locally	YesScan data is processed locally on your PC. You use an Access Token to unlock your Scan file.	NoThe encrypted Scan file is sent to SekChek for processing where your security controls are assessed and benchmarked against the industry average.
Analyses all user and		

group accounts, not sample-based	Yes	Yes
Fast turnaround time	YesYour report is available within minutes of completing a Scan.	YesYour report is typically despatched within 12 hours of receipt of your Scan file.
Report format	MS-Access database with a user-friendly interface.	MS-Word (main report), MS-Excel (option for large report sections).
Easy to read results	YesResults are presented in graphical and tabular formats. Each Report database includes a comprehensive set of summary and detailed reports.	YesEach report section contains a graphical summary and detailed results.
Overall Rating of security on a system	No	YesSecurity is rated against real-life industry averages for security.
Independent, objective reporting	YesThe results are the same regardless of who performs the Scan	YesThe results are the same regardless of who performs the Scan
Comparisons against real-life industry averages and leading practices for security	Yes	Yes
Ability to compare security of two systems	YesComparisons can span both time and system.	YesComparisons can be made for a system at different points in time.
Scan data can be queried, sorted, copied / pasted	YesScan data is written to a Report database in MS- Access format.You can view the results via SekChek's comprehensive set of reports or develop your own queries using	LimitedOutput is typically in MS-Word format.

	MS-Access' powerful data manipulation utilities.	
Reports provide Implications and general Recommendations	NoHowever, a comprehensive glossary of all reported security properties is included.	Yes
Embedded security tools & utilities	YesFree utilities include: A tool that performs a basic audit of a client PC; a SID resolver; a redundant SID locator; Encryption /Decryption software; Ping; file hashing software; and a Service Request sub- system for requesting popular documents.	YesFree utilities include: A tool that performs a basic audit of a client PC; a SID resolver; a redundant SID locator; Encryption /Decryption software; Ping; file hashing software; and a Service Request sub- system for requesting popular documents.
Access to SekChek's Technical Support Helpdesk	Yes	Yes
Money-back guarantee (no report, no charge)	Yes	Yes
A proven track record	YesThe tool builds on the strengths of the classic SekChek tool	YesSekChek has provided this service to leading audit firms, security practitioners and internal audit functions in the world's best known organisations since 1996.

If you make frequent use of SekChek, why not enquire about our generous discounts for subscription and volume purchases.

Clients & Users

Countries & Regions

SekChek is used by international audit firms, ERS consultants, IS professionals, internal auditors, security consultants & general management in 140 countries.

Many large and well known multinationals have used the tool to centralize security reviews of systems located at their overseas offices and subsidiaries.



Major Industries

SekChek's client-base includes service organisations and <u>large multi-nationals</u> as well as many smaller niche companies. Our clients span all major industry sectors from financial services, to manufacturing, public utilities, and government.

A unique statistics database permits SekChek to calculate real/actual industry averages for security. As new reviews are processed, summaries of the results (excluding client identification) are automatically added to a dynamic database of over 80,000 assessments.

This allows you to see how well your security compares with other companies in your industry sector.



Contact Details



Please direct all enquiries (pricing, subscriptions, passwords, technical issues & problems) on *SekChek* to:

- E-mail: <u>inbox@sekchek.com</u>
- <u>http://www.sekchek.com</u>

Service Hours

Monday to Friday 04:00 to 18:00 GMT

What's New?

<u>Expand all</u> <u>V5.1.4 (26-Jun-2017)</u>

SekChek Client software

- Improved support for Windows 10, including new audit categories
- Cater for secure https access to SekChek's web site
- General maintenance

SekChek for Active Directory and Windows:

- Enhancements for Server 2016, including new audit categories
- General maintenance

SekChek for OS/400 and UNIX: Minor maintenance.

SekChek for Netware: No further enhancements. The tool is provided on an 'as is' basis.

V5.1.3 (24-May-2016)

SekChek Client software

- Embedded a new digital certificate in the software. The certificate is valid to 17 July 2018, thumbprint = 133a91efed3b2a046506519fdb40e515062fe77a.
- General maintenance

SekChek for Active Directory and Windows:

- Enhancements for Server 2012 R2
- General maintenance

SekChek for OS/400 and UNIX: Minor maintenance.

SekChek for Netware: No further enhancements. The tool is provided on an 'as is' basis.

V5.1.2 (25-May-2015)

SekChek Client software

• Enhancements for Windows 10

SekChek for Active Directory and Windows:

- Enhancements for Server 2012 R2
- Scan new properties on an LDAP server
- Scan new properties on a Hyper-V server

SekChek for OS/400 and UNIX: Minor maintenance.

SekChek for Netware: No further enhancements. The tool is provided on an 'as is' basis.

<u>V5.1.1 (10-Jul-2014)</u>

SekChek Client software

- Embedded a new digital certificate in the software. The certificate is valid to July 2016.
- Improved encryption logic so that it identifies and corrects bad file names

SekChek for Active Directory and Windows:

- Enhancements for Server 2012 R2
- Scan 5 new properties of the LDAP server
- Detect whether host is a Hyper-V server

SekChek for OS/400 and UNIX: Minor maintenance.

SekChek for Netware: No further enhancements. The tool is provided on an 'as is' basis.

V5.1.0 (08-Nov-2013)

SekChek Client software

- PC Auditor tool: Report on User Account Control (UAC) settings
- Cater for Office 2013 file formats (Word, Excel, Access)
- Improved the installation routine for SekChek's digital certificates

SekChek for Active Directory and Windows:

- Scan permissions on Network shares
- Report on Task Scheduler configuration
- Report on User Account Control (UAC) setting
- Improved the reliability of reporting on the Password Complexity and Reversible Password Encryption controls for standalone servers

SekChek for OS/400 and UNIX: Minor maintenance.

<u>V5.0.9 (07-Jun-2013)</u>

SekChek Client software

- Prevent the encryption process from freezing if a Scan file's header is corrupt.
- PC Auditor tool: Report on advanced audit settings, registry size

SekChek for Active Directory and Windows:

- Scan advanced audit settings (from Server 2008 R2)
- System Configuration report section: Added domain Sid, registry size, regional language settings
- Report on 53 advanced audit settings if the host is using advanced auditing features
- Report on non-existent members of local groups (deleted accounts)
- Improved reporting for Password Setting Objects (PSOs)
- Improved the handling of situations where the output Scan file is locked by a host's anti-virus software

SekChek for OS/400 and UNIX: Minor maintenance.

V5.0.8 (14-Jan-2013)

SekChek Client software: Updated the folder selection form to include network folders.

SekChek for Active Directory and Windows:

- Made changes to cater for Windows 8 / Server 2012 and Server Core.
- System Configuration report section: Added Windows Firewall settings.
- QFE, hot-fixes report section: Included settings for Windows Updates (WSUS).
- Added new analyses for internal system accounts and Windows Role and Features.

SekChek for OS/400 and UNIX: Minor maintenance.

V5.0.7 (16-Jul-2012)

- Embedded a new encryption certificate in the software. The certificate is valid to July 2014.
- Refreshed the sample reports to reflect enhancements made over the last few months. PDF versions of all sample reports are available on SekChek's web site.
- *SekChek* for Windows: Include Read Only Domain Controllers (RODCs) in the scan list when the option to query all DCs for users' last logon times is selected.
- *SekChek* for Windows: Ensure the full text for user login notifications is extracted. The text was previously truncated after 500 characters.
- *SekChek* for UNIX: Minor maintenance.
- Tools Menu. Converted the output HTML files from the utilities on SekChek's tools menu to Unicode format. This ensures foreign characters, such as Chinese, Japanese and Russian are properly displayed.
- Tools Menu. Added several new properties to the Query Active Directory tool.

V5.0.6 (01-Oct-2011)

Added 7 new utilities to the <u>Tools menu</u>:

- *Create File Hash*. Displays the sha1 hash value for a file.
- *Windows Firewall Auditor*. Displays Windows Firewall's configuration settings, profiles, currently active rules and all Inbound / Outbound rules.
- *List Missing Windows Updates*. Highlights Windows updates not installed on your PC.
- List Installed Products. Lists MSI-installed products on your PC.
- *Search Event Log.* Queries the Windows Event log for Error and Warning Events.
- *Query File Permissions*. Lists Discretionary Access Control Lists (DACLs) defined on files and folders on local and remote systems.
- *List Open File Shares*. Displays open shared files on a target server.

SekChek for Active Directory:

• Improved the accuracy of last logon times for domain user accounts. The Scan process now uses a property available from Server 2003, which is replicated across Domain Controllers (DCs) every 14 days, compares this value with the last logon property (not replicated) on the DC being scanned, and uses the most recent of the 2 values.

If you need even more accuracy (the absolute latest last login times), you must select the run-time option that forces SekChek to query all DCs in the domain.

SekChek for Active Directory and Windows:

• List File Permissions (DACLs) report. Improved the resolution of: SIDs to Domain\Account names; and a domain name of BUILTIN for a trustee to the trustee's actual domain or machine name.

The main SekChek software: Improved the Help file

V5.0.5 (20-Dec-2010)

Added 3 new utilities to the Tools menu:

- *PC Auditor*, which performs a basic analysis of your local computer system and displays the results in your Internet browser.
- *Find orphaned SIDs*, which searches NTFS for Security Identifiers (SIDs) that may belong to old security accounts that no longer exist
- *Resolve SID*, which resolves a SID and presents it in a user friendly format (System name \ Account name)

SekChek for Windows:

- Added an option to analyse an MS-Exchange Server: Organization, Servers, Databases, Storage groups, Users
- Analyse software installed by Windows Installer (MSI)
- Analyse system-wide, quick-fix engineering (QFE) updates applied to the Windows OS
- Analyse attribute 'Is Object Protected Against Deletion', which is defined on several object types
- Reduced the risk of the Scan process failing due to anti-virus software locking the output files

V5.0.4 (14-May-2010)

- Added a utility that lists properties for an Active Directory account. The utility is particularly useful because it displays properties that are not visible in Windows' GUI. See Main Menu | Tools | Query Account Property.
- Renewed *SekChek's* embedded certificate (public key) with a new certificate that is valid until April 2013. *SekChek* will prompt you to install the new certificate during the installation process.
- *SekChek* for Windows: Scan domain for Password Setting Objects (PSOs), which were introduced in Server 2008.
- *SekChek* for Windows: Included 14 additional properties in the Scan process, including functionality levels for the DC and Forest and DEP settings.
- *SekChek* for UNIX: Minor maintenance.

V5.0.3 (23-Oct-2009)

• Added a Ping utility to the Tools menu. The utility is useful for analysing

network connectivity issues.

- *SekChek* for Windows: Included System Config details in the Scan. This information supports a new report section containing properties for the following objects: Computer; Operating System; Processors; BIOS; Page files; Network adapter; and Motherboard.
- *SekChek* for Windows: Scan domain for Global Catalog Servers.
- *SekChek* for Windows: Scan 'password complexity' and 'store passwords with reversible encryption' controls on member Servers.
- *SekChek* for Windows: Improved the code that binds to an Active Directory domain. Try 1) Domain's Netbios name; 2) Domain's DNS name; 3) Host machine's DNS name.

<u>V5.0.2 (18-Jun-2009)</u>

- Added the ability to view the digital signature on the SekChek software (SekChek.exe).
- Help file: Updated images and implemented various improvements.
- *SekChek* for Windows: Check whether the account used to run the Scan process has sufficient privileges to access the system's Policy object *before* the Extract process is started. This will prevent delays and the need for reruns due to incomplete Extract data.
- *SekChek* for Windows: Ensure SekChek always binds to the *target machine's* domain instead of the *authenticated user's* domain. This allows the Scan to be run from an Administrator account in any trusted domain, as long as the account has sufficient privileges to Scan the target domain.
- *SekChek* for UNIX: Added several new policies to the Scan function.

V5.0.1 (14-Jan-2009)

- Added Word 2007 to the list of report format options.
- *SekChek* for AS/400: Report on Object and Data Authorities for 6 additional OS/400 commands (STRSQL, UPDDTA, SAVOBJ, RSTOBJ, SAVLIB, RSTLIB).
- *SekChek* for AS/400: Improved support for far eastern characters.
- *SekChek* for UNIX: Improved support for NFS mounted volumes on most UNIX variants.
- *SekChek* for Windows: Cater for read-only domain controllers. Previous

versions of SekChek do not recognise this new type of DC.

• *SekChek* for Windows: Reduce the risk of a Scan terminating if it cannot access a group member due to insufficient permission.

V5.0.0 (07-May-2008)

- Released the <u>SekChek Local</u> range of products.
- Improved validation of the Extract / Scan files during the encryption process.
- Removed password length restrictions for the SekCrypt utility.
- Fixed a problem where, under certain conditions, the software incorrectly issued a message stating that PKI features are not supported by the system.
- Help: Improved FAQs and removed old, redundant references.

Check our web-site for the <u>latest news</u> and updates.

Getting Started with SekChek

If you are new to *SekChek* we recommend you start by familiarising yourself with the basic process:

- **1. Creating** the Scan software
- **2. Executing** the Scan software on the computer system you want to analyse
- 3. Encrypting the file from the Scan process
- 4. Emailing the encrypted Scan file to SekChek for processing
- 5. Decrypting your *SekChek* report package

A good source of information is the Help section called 'Overview of the process' for the system type that interests you. For example, take a look at: <u>SekChek for Windows</u>.

Step 1

The first step is to define your personal processing options (Options / User Preferences / General Tab). To ensure your Scan data is adequately protected we recommend you enable the '<u>Use Public Key Encryption</u>' option.

Step 2

After creating the *SekChek* for Windows Scan software, try running it on your own PC. *SekChek* will run for a few seconds and generate an encrypted Scan file.

Step 3

If your organisation is new to *SekChek* and you want to see what a *SekChek* report looks like for your particular environment, contact our <u>Helpdesk</u> and ask for a free trial.

What if I get stuck?

Try searching *SekChek's* Help file and the list of Frequently Asked Questions (FAQs) for the answer to your question.

If you are in the middle of a process and you are not sure what to do next, try dragging a SekChek file onto *SekChek's* main menu. *SekChek* will prompt you with the next step.

If you are still stuck, don't worry. You can always contact our <u>Helpdesk</u> and ask one of our support technicians to talk you through the process.

What does the SekChek software contain?

The *SekChek* Client software contains everything you need to evaluate security on most types of computer systems and to compare your controls against industry averages and leading international practices for security.

This includes:

- Software to scan security settings on most types of computer systems.
- Comprehensive Help and instructions to guide you through the process.
- Specialised encryption software to ensure your Scan data is securely protected.
- **Sample reports** for all platforms supported by *SekChek*.

• The **SekCrypt** utility; a general purpose file encryption tool that uses industry standard encryption algorithms, such as DES and AES.

• A **File Splitter** utility that splits large files into a collection of smaller files and joins them back together. This is useful when you want to break up a large file before transmitting it via email.

• A **Service Request** utility; allows you to submit automated requests (emails) for common information to *SekChek*.

• A **version-checker** utility to ensure you always have access to the latest version of the *SekChek* software.

The Main Menu Tool Bar

SekChek for Windows						
File	View	Options	Tools	Help		
\square	A	S/400	Ţ		Netware	

The bar at the top of SekChek's main form provides access to the following submenus:

- File Menu
- <u>View Menu</u>
- Options Menu
- Tools Menu
- <u>Help Menu</u>

View Menu



Certificates: Check Digital Signature on EXE

Checks the digital signature on the SekChek software to confirm that the file has not been tampered with. The function also shows the time the software was signed and the hash and encryption algorithms that were used.

Certificates: View Signing Certificate

Displays the certificate used to sign all software published by SekChek.

Log File

Opens SekChek's logfile. The logfile is useful for error diagnostic purposes.

Sample Reports...

Opens sample audit reports for AS/400, Active Directory, Windows Server and UNIX. The latest versions of sample reports are published on our web-site at www.sekchek.com/Reports.htm

Options Menu

😨 SekChek f	or W	lindows	
File View	Opt	ions Tools Help	
		User Preferences	
		Always On Top	Ctrl+T
-1. Create	✓	Check for Software Updates on Load (default ON)	
Create Sca	USU	Itware for execution on a windows server or uomain	Create

User Preferences

This is where you define personal preferences, such as your contact details, runtime options and report formatting requirements. The settings are remembered between sessions and software upgrades, so you only have to define them once.

Always On Top

Ensures that SekChek's main form is not hidden behind other forms. This is useful when dragging / dropping files onto the main menu.

The default value is OFF.

Check for Software Updates on Load

Queries www.sekchek.com for updates to the SekChek software each time you start SekChek. Prompts to download and update SekChek if a later version exists.

The Options Screen

The Purpose of this Screen

This screen allows you to define personal preferences & particulars, such as your contact details & report formatting requirements. The values that you enter via this screen are *remembered* between sessions, so you only have to define them once.

	City/Office:	(between 8 & 25 characters)
Bradley Govender	London	*********
elephone Number:	Country:	Show Password
+44 (23) 123 4567	UK	Use Public Key Encryption
	Customer Code: SEK	K001 Generate Complex Password
want all report sections greate	r than 10000	lines in an MS-Access database
		<u>C</u> hange
C:\SekChek Files		

What Are General Options Used For?

Your Option settings are used as default values each time you create a copy of the Scan software or encrypt a *SekChek* file.

The values are embedded in the Scan software and the encrypted Scan files you send to us for processing. This includes *SekChek* for Windows and NetWare,

where the encryption is done on the target system.

The information you enter helps us to identify the owner of a file, influences the behaviour of the Scan software and provides us with the instructions we need to ensure your report is processed in the required format. Note that these values can be overridden during the Scan and Encryption processes.

General Options

General Options

Name and City/Office/Country

This is the name of the person requesting the *SekChek* service. E.g. John Smith, Seattle, USA

Telephone Number

This is required so we can contact you in the event that we encounter problems or require clarification from you. Please use the international format for telephone numbers. E.g. +44 (171) 936 3000

Customer Code

Your customer/account code (6 characters) for *SekChek* Services. Leave as '<---->' if you don't know your customer code and we will enter it for you.

Encryption Password

The password will be automatically included inside the encrypted package containing your Scan data. This password is not used to encrypt your Scan files, but is used to encrypt your *SekChek* reports. SekChek will require you to select a complex password consisting of at least 8 alpha-numeric characters. E.g. 1Lettuce4U

Public Key Encryption

This option enables *SekChek's* Public Key encryption features. These features ensure that your Scan files and reports are securely encrypted with industry-

standard encryption algorithms, such as RSA and DES. We recommend that you turn this option on.

For more information refer to <u>Public-Private Key Encryption</u>.

Preferred Report Format

Specify the format you require your *SekChek* reports in. E.g. Word 2007.

Paper Size

In general, Letter size stationery is used in the US & Canada & in some South American countries; A4 is mostly used in Europe, Australia, Far Eastern countries & in Africa.

Spelling

Specify English US or English UK. Examples of differences in spelling are:

- English US color, summarize;
- English UK colour, summarise.

Large Report Options

Some *SekChek* reports can be very large, so we provide you with 2 options for handling report sections with a large number of lines. We can put large report sections in:

- An MS-Access database; or
- An Excel spreadsheet.

For example, if you request 'All report sections greater than 100 lines in an Excel document' the main report will be in Word format and report sections with less than 100 lines will be written to the document as Word tables. However, report sections with more than 100 lines will be written to Excel and the main Word

document will contain hyper-links that point to the sections in Excel.

If you request 'All report sections greater than 0 lines in an Access document' the main report will be in Word format and *all* detailed report sections will be written to an Access document. The main Word document will contain hyper-links that point to the sections in Access.

Produce Summary Document

Click on (check) to request a summary document containing an Overall Rating of security against the industry average and a consultant's comments on the report.

Default Path

You can enter a path that *SekChek* will initially default to for functions such as encrypting and decrypting Scan files and reports, and creating copies of Scan software.

Notification Request: Receive my Scan file

Instructs SekChek to notify you via email to confirm that we have received your Scan file.

Notification Request: Return my Report package

Instructs SekChek to notify you via email to confirm that your encrypted Report package has been despatched to you.

Notification Request: Delete my Scan data and Report...

Instructs SekChek to notify you via email as soon as your Scan data has been

deleted from our system.

Do not store my password in clear text

By default SekChek writes your password to its INI and log files in clear text format. Turn on to ensure your password is stored in a scrambled format. This serves as a mild deterrent against casual or inquisitive intruders.

System / Client Specific Options

These are your default processing options for SekChek reports. Leave blank if you work at many clients and the values are likely to be different for each SekChek analysis that you run.

Client Details The name of your (or your client's) org	ganisation:	Evaluation Options
My Client Ltd.		Standards Template Nbr: 0
Country where the Host is located:	Industry type:	Compare security against:
Bahamas	Financial Services	Financial Services
Charge (DIS) code: My Internal Code		
Notes:		
These are your default processing op 1. Create the Windows & Netware Sca 2. Encrypt AS/400 and UNIX Scan files	ions for SekChek reports. They are d an software. s.	displayed each time you:

The System / Client specific options are used in the following functions:

- Creation of Windows & Netware Scan software. (Optional)
 If defined, the options are embedded in the Scan EXE as default values; they can be changed at execution time.
- The final values are embedded in the encrypted Scan file. 2. Encryption of AS/400 and UNIX Scan files. (Mandatory)

The options are embedded in the encrypted Scan file.

The name of your (or your client's) organisation

This is the name of your (or your client's) organisation where the SekChek Scan

is being run. This name will appear in your SekChek report.

Country where the Host is located

The location of the Host system that is being analysed. Used for statistical purposes.

Industry type

The industry type that best describes the client's business. Used for statistical purposes.

Charge / DIS code

Optional. This is your own internal charge code. It is useful for keeping track of SekChek usage and for internal billing purposes.

Compare against industry

The industry type (e.g. Manufacturing) against which you want to compare the Host's security controls. Select <All industry types> to compare security against security averages for all industries.

Standards template number

The number of the template containing client-specific security values that you have registered with SekChek. If specified, we will use the security values in the template, rather than SekChek's leading practice values, when we process your report. Leave as 0 to use SekChek's default values.

Tools Menu

SekChek's Tools

These security tools and utilities are provided free of charge for use on your local PC only. No license is required to use any of these tools. You are free to distribute them in their current form to anyone you wish.



Encrypt / Decrypt File

Encrypts or decrypts a file.

File Splitter

Splits any large file into a collection of smaller files. You can control the size of the output files in the range 10,000 (10KB) to 10,000,000 (10MB). The default size is 2,500,000 bytes.

Smaller files can speed up the transmission process and allow you to bypass any file size restrictions that may exist on your firewall. A general recommendation is that you should consider splitting Scan files larger than 5MB into several smaller files of 2MB (2,000,000) each.

To join a file that has been split using the *SekChek* File Splitter Utility, select one of the split-file collection... Click Join.

Note: When joining split-files, ensure that the full collection of split-files is present in the same directory.

Create File Hash

Calculates and displays the sha1 hash (digest) value for a file.

You can also use the tool to compare a file's saved hash value with the file's hash value at a later point in time. This can be used to determine whether a file has been modified.

More information: www.sekchek.com/Free-Tools-File-Hasher.htm

PC Auditor

The tool will perform a basic analysis of your system and display the results in your Internet browser. The scope of the analysis includes the current user and computer, disks, local security accounts, and your system's Regional and Language Options.
Note: To ensure correct results you must execute the SekChek software with Administrator privileges. I.e. 'Run As Administrator'.

More information: <u>www.sekchek.com/Free-Tools-PC-Auditor.htm</u>

Windows Firewall Auditor

Displays security configuration settings defined in Windows Firewall with Advanced Security (available from MS Vista). The scope of the analysis includes:

- The Firewall's Domain, Private and Public profiles
- The currently active Firewall rules
- Inbound rules
- Outbound rules

More information: <u>www.sekchek.com/windows-firewall-report.htm</u>

List Missing Windows Updates

The utility lists Windows Updates and hot fixes not installed on your PC by searching Microsoft.com for eligible updates.

More information: <u>www.sekchek.com/missing-windows-updates-report.htm</u>

List Installed Products

Lists products installed on your PC by Microsoft Installer (MSI).

More information: <u>www.sekchek.com/MSI-installed-products-report.htm</u>

Search Event Log

The utility queries Windows' Application and System Event logs for Error and Warning Events. It can also search for a specific Event code.

More information: <u>www.sekchek.com/query-event-log-report.htm</u>

Query Active Directory

The utility queries any Active Directory object and returns the value defined for the chosen property. Valid object types include users, groups, computers and containers. The utility is particularly useful because it displays properties that are not visible in Windows' GUI.

Notes:

- The name of the object to query must be specified in LDAP format. E.g. CN=Administrator,CN=Users.
- For those properties that Windows does not replicate across domain controllers (indicated by 'NR'), there is an option to query all DCs in the domain in order to retrieve the property's latest, most current value.
- If you are not sure of an object's name, you can perform a wild-card search of Active Directory using part of its name.

More information: <u>www.sekchek.com/Free-Tools-Query-AD.htm</u>

Query File Permissions (DACLs)

The tool queries Discretionary Access Control Lists (DACLs) defined on files and folders on local and remote systems. It lists an object's attributes and all Access Control Entries (ACEs) in the DACL.

More information: <u>www.sekchek.com/free-tools-list-dacls.htm</u>

Resolve SID

The tool will resolve any valid security identifier (SID) to its friendly name. E.g. S-1-5-32-544 to BUILTIN\Administrators.

If the SID is not found in your current domain, it will try to resolve the SID by searching all trusted domains.

Find Orphaned SIDs in NTFS

The utility lists orphaned security identifiers (SIDs) defined on files and directories in the NT file system (NTFS). Orphaned SIDs typically belong to security accounts that no longer exist on your system.

The utility searches all Owner and Trustee records defined on files and directories in the selected search path. Search results include permissions that are inherited from a higher level in NTFS

More information: www.sekchek.com/Free-Tools-Sid-Locator.htm

List Open File Shares

Lists open shared files on a target Server, including details of the file's users and the file's open mode.

More information: www.sekchek.com/free-tools-list-open-files.htm

Ping Computer

The utility pings a computer or domain to test network connectivity. Valid address formats are: NetBios, DNS (FQDN) and IP address.

Help Menu

le View Options Tools He	elp
AS/400	Help Contents and Index F1
1. Create Scan Software Create Scan software for exec	What's New? Frequently Asked Questions Getting Started
-2. Run the Scan Scan security on a Windows se	Go to www.SekChek.com Contact SekChek Check for Updates

Help Contents and Index

Opens SekChek's Help system. You are viewing this now.

What's New?

Displays a summary of new features and enhancements introduced in recent versions of the SekChek software.

Frequently Asked Questions (FAQs)

Provides answers to the most common questions asked about the SekChek software and service.

For more information see: www.sekchek.com/faq.htm

Getting Started

Provides some useful tips to get started with SekChek. This is a good starting point if you are new to the service.

Go to SekChek.com

Takes you to the home page on our web-site: <u>www.sekchek.com</u>.

Contact SekChek

Our contact information: service hours; our common email address; telephone numbers; and postal address.

Check for Updates

Checks our web-site for updates to the SekChek software. If a later version is available you will be prompted to download the new version.

About SekChek

Displays general information for the SekChek software and your system, such as SekChek's version number, your system's name, IP address, current memory usage.

Overview



We provide you with:

- Detailed step-by-step instructions for all processes;
- Software to encrypt & decrypt the transmitted files.

Creating the Scan Software

The Scan software is used to scan security on an AS/400 machine.

You can create a copy by clicking on the button *Create Scan software*.

SekChek for AS/400		
le View Options Tools	Help	
AS/400	Netware	UNIX
- 1. Create Scan Software	cution on a OS/400 system	Create
2. Run the Scan		

Next Step...

Scanning Security on an AS/400 Machine

Scan Instructions

Introduction

You have a choice of 2 methods for scanning security information on an AS/400 computer:

Manual Method

Requires you to enter a series of commands via the OS/400 command line. It takes a little longer (20-30 minutes) to scan the security data, but is less 'intrusive' than the automated method.

The manual method is best suited to environments where it is not desirable to load software onto the AS/400 machine.

Automated Method

Involves transferring the Scan Software to the AS/400 machine, compiling and executing it. It is slightly quicker than the manual method, but is more 'intrusive'.

Although the software is removed from the AS/400 computer at the end of the scan process and the Source (CL) code may be inspected, this method is not recommended if there is sensitivity about compiling and running software on the AS/400.

Detailed instructions for both Scan methods are provided. The only difference in

the results is that the automated method will analyse authorities for more OS/400 commands than the manual method.

Scan Instructions (Manual Method)

Prerequisites

None.

Outline of this Step



****IMPORTANT****

To ensure correct results use the QSECOFR profile for the following operations. The user profile used will be locked while the DSPPGMADP command below is running. If this profile owns a lot of objects, the profile could be locked for an extended period of time

Refer to IBM Technical APAR#: SA54337 for further information. We recommend that command DSPPGMADP is run during off-peak hours.

1. Allocate Temporary Library

From the AS/400 command line enter:

CRTLIB LIB(SEKCHEK)

SekChek = Desired Output Library Name

2. Dump User Profiles (basic information) to a File

From the AS/400 command line enter:

DSPUSRPRF USRPRF(*ALL) TYPE(*BASIC) OUTPUT(*OUTFILE) OUTFILE(SEKCHEK/PROFBAS)

SEKCHEK = Output Library Name PROFBAS = Output File Name

3. Dump the System Values to a Spooled File

From the AS/400 command line enter:

WRKSYSVAL SYSVAL(*ALL) OUTPUT(*PRINT)

4. Create a Physical File to contain the Spooled File created in Step 3

From the AS/400 command line enter:

CRTPF FILE(SEKCHEK/SYSVALS) RCDLEN(132)

SEKCHEK = Output Library Name SYSVALS = Output File Name

5. Copy the Spooled File to the Physical File created in Step 4

From the AS/400 command line enter (e.g. see notes below):

CPYSPLF FILE(QSYSPRT) TOFILE(SEKCHEK/SYSVALS) JOB(012345/MYUSER/MYUSER2S1)

SEKCHEK = Output Library Name SYSVALS = Output File Name 012345 = Job Number for the Spooled File created in step 3 MYUSER = User Name for the Spooled File created in step 3 MYUSER2S1 = Job Name for the Spooled File created in step 3 [Use 'WRKOUTQ' (display attributes option) or 'WRKSPLF' command to obtain information about the Spooled File]

6. Dump Program Adopt Authorities to a File (optional step)

This (optional) step will dump a list of all programs that adopt the authorities of the QSECOFR & QSYS profiles.

From the AS/400 command line enter:

DSPPGMADP USRPRF(QSECOFR) OUTPUT(*OUTFILE) OUTFILE(SEKCHEK/PGMADP)

SEKCHEK = Output Library Name QSECOFR = Profile being adopted PGMADP = Output File Name

From the AS/400 command line enter:

DSPPGMADP USRPRF(QSYS) OUTPUT(*OUTFILE) OUTFILE(SEKCHEK/PGMADP) OUTMBR(*FIRST *ADD)

SEKCHEK = Output Library Name QSYS = Profile being adopted PGMADP = Output File Name

This command will *append* the output to file PGMADP created by the previous command.

7. Dump Object Authorities for Specific Objects to a File (optional step)

This (optional) step will dump a list of object authorities for the object STRDFU (a powerful data manipulation utility).

From the AS/400 command line enter:

DSPOBJAUT OBJ(QSYS/STRDFU) OBJTYPE(*CMD) OUTPUT(*OUTFILE) OUTFILE(SEKCHEK/OBJAUT)

STRDFU = Object for which a list of object authorities is required *CMD = Object type SEKCHEK = Output Library Name OBJAUT = Output File Name

You can dump the object authorities for as many objects as you wish. The 'OUTMBR' parameter ensures that the data is appended (added) to file OBJAUT. From the AS/400 command line enter:

DSPOBJAUT OBJ(QSYS/ObjectName) OBJTYPE(*ObjectType) OUTPUT(*OUTFILE) OUTFILE(SEKCHEK/OBJAUT) OUTMBR(*FIRST *ADD)

QSYS = Name of the library containing the object *ObjectName* = Name of the object for which a list of authorities is required *ObjectType* = Object type (e.g. *CMD - command, *PGM - program) SEKCHEK = Output Library Name OBJAUT = Output File Name

This command will *append* the output to file OBJAUT created by the previous command.

8. Dump Profiles with Default Passwords to a Spooled File (optional step)

From the AS/400 command line enter:

ANZDFTPWD ACTION(*NONE)

9. Create a Physical File to contain the Spooled File created in Step 8 (optional step)

From the AS/400 command line enter:

CRTPF FILE(SEKCHEK/ANZDFTPWD) RCDLEN(132)

SEKCHEK = Output Library Name ANZDFTPWD = Output File Name

10. Copy the Spooled File to the Physical File created in Step 9 (optional step)

From the AS/400 command line enter (e.g. see notes below):

CPYSPLF FILE(QPSECPWD) TOFILE(SEKCHEK/ANZDFTPWD) JOB(012345/MYUSER/MYUSER2S1) SPLNBR(*LAST)

SEKCHEK = Output Library Name ANZDFTPWD = Output File Name 012345 = Job Number for the Spooled File created in step 8 MYUSER = User Name for the Spooled File created in step 8 MYUSER2S1 = Job Name for the Spooled File created in step 8 [Use 'WRKOUTQ' (display attributes option) or 'WRKSPLF' command to obtain information about the Spooled File]

11. Dump Service Table to a Spooled File (optional step)

From the AS/400 command line enter:

WRKSRVTBLE SERVICE(*ALL) OUTPUT(*PRINT)

12. Create a Physical File to contain the Spooled File created in Step 11 (optional step)

From the AS/400 command line enter:

CRTPF FILE(SEKCHEK/SRVTBLE) RCDLEN(132)

SEKCHEK = Output Library Name SRVTBLE = Output File Name

13. Copy the Spooled File to the Physical File created in Step 12 (optional step)

From the AS/400 command line enter (e.g. see notes below):

CPYSPLF FILE(QSYSPRT) TOFILE(SEKCHEK/SRVTBLE) JOB(012345/MYUSER/MYUSER2S1) SPLNBR(*LAST)

SEKCHEK = Output Library Name SRVTBLE= Output File Name 012345 = Job Number for the Spooled File created in step 11 MYUSER = User Name for the Spooled File created in step 11 MYUSER2S1 = Job Name for the Spooled File created in step 11 [Use 'WRKOUTQ' (display attributes option) or 'WRKSPLF' command to obtain information about the Spooled File]

14. Download the Scan Files to a PC

Download files <u>PROFBAS</u>, <u>SYSVALS</u> and (if created) <u>ANZDFTPWD</u>, <u>PGMADP</u>, <u>OBJAUT</u> & <u>SRVTBLE</u> to a PC.

****IMPORTANT****

Specify binary in your copy utility or ftp software when downloading the PROFBAS file to a PC. For all other files, specify fixed-length records and ASCII/text format.

Basic ftp commands are:

ftp 193.241.02.85 (establish an ftp connection with machine 193.241.02.85) *Note: Remember to replace 193.241.02.85 with the relevant IP address on your system.*

get sekchek/profbas *local_filename* (copy the *profbas* file from the remote machine to the default directory on the local machine. The *local_filename* in this case would be *Profbas.txt* in a specified directory on the PC)

binary (switch to binary transfer mode)

ascii (switch to ASCII transfer mode)

bye (or **quit**) (exit ftp)

More information: <u>A sample ftp session</u>

15. Delete Temporary Files Created on AS/400

From the AS/400 command line enter:

RMVLIBLE SEKCHEK

DLTLIB LIB(SEKCHEK)

This will delete library SEKCHEK and its contents (i.e. all files/objects created

during the Scan process).

Should you encounter difficulties with the process, call us with details of the problem and we will help guide you through the process.

Next Step...

Encrypt the Scan Files on your PC

Scan Instructions (Automated Method)

Prerequisites

You should already have <u>created a copy of the Scan software</u>

Outline of this Step



****IMPORTANT****

To ensure correct results use the QSECOFR profile for the following operations. The user profile used will be locked while the DSPPGMADP command, within the CL script, is running. If this profile owns a lot of objects, the profile could be locked for an extended period of time

Refer to IBM Technical APAR#: SA54337 for further information. We recommend that the SekChek for AS400 CL script is run during off-peak hours.

1. Allocate Temporary Library

From the AS/400 command line enter:

CRTLIB LIB(SEKCHEK)

SEKCHEK= Desired Output Library Name

2. Allocate Source File in Temporary Library

From the AS/400 command line enter:

CRTSRCPF FILE(SEKCHEK/SEKASSRC) MBR(SEKASEXT)

SEKCHEK= Library to contain the Scan Source SEKASSRC= Source File Name SEKASEXT= Member in Source File

(Optional) To verify that the Library, File and Member have been created successfully, from the AS/400 command line enter:

DSPPFM FILE(SEKCHEK/SEKASSRC) MBR(SEKASEXT)

If either the Library, File or Member objects do not exist on the AS/400 system, an error will be displayed with details of which object does not exist.

Possible Errors:

- Library *<LibraryName* > Not Found
- File *<FileName>* in Library Not Found
- File *<FileName>* in Library *<LibraryName>* with Member *<MemberName>* Not Found

3. Copy the Scan Software Source to the AS/400

Copy file SEKASEXT from the Scan Software diskette/PC to file SEKASSRC member SEKASEXT in Library SEKCHEK.

Basic ftp commands using a machine with sample IP address 193.241.02.85:

ftp 193.241.02.85 (establish an ftp connection with machine 193.241.02.85)

put *local_filename* **sekchek/sekassrc.sekasext (replace)** (copy *local_filename* from the default directory on the local machine to the default directory on the remote machine with replace existing files set to on)

bye (or quit) (exit ftp)

More information: <u>A sample ftp session</u>

4. Compile the Scan Software (CL) Source

From the AS/400 command line enter:

CRTCLPGM PGM(SEKCHEK/SEKASPGM) SRCFILE(SEKCHEK/SEKASSRC) SRCMBR(SEKASEXT) USRPRF(*OWNER)

SEKCHEK= Library Name SEKASPGM= Executable Program Name SEKASSRC= Scan Software (CL) Source File SEKASEXT= Scan Software (CL) Source Member

5. Execute the Scan Software (SEKASPGM)

To run the Scan software interactively, enter the following command from the

AS/400 command line:

CALL PGM(SEKCHEK/SEKASPGM)

SEKCHEK= Library Name SEKASPGM= Scan Program Name

Files <u>PROFBAS</u>, <u>SYSVALS</u>, <u>OBJAUT</u>, <u>PGMADP</u>, <u>ANZDFTPWD</u>, <u>SRVTBLE</u> & <u>SEKLOG</u> will be written to library SEKCHEK.

Note that file SRVTBLE, which contains details of the services table, will not be created if the Scan software is executed in batch mode (see below).

This is because the underlying command is not supported by OS/400 in this mode, so you will receive an error message (CPD0031 "Command WRKSRVTBLE not allowed in this setting") at execution time. All other files will be created OK. In general, we recommend SekChek is run interactively, rather than in batch mode.

To run the Scan software in batch mode, enter the following command from the AS/400 command line:

SBMJOB CMD(CALL PGM(SEKCHEK/SEKASPGM)) JOB(SEKCHEK)

SEKCHEK= Library Name SEKASPGM= Scan Program Name SEKCHEK= Job Name

6. Download the Scan Files to a PC

Download files <u>PROFBAS</u>, <u>SYSVALS</u>, <u>ANZDFTPWD</u>, <u>PGMADP</u>, <u>OBJAUT</u>, <u>SRVTBLE</u> and <u>SEKLOG</u> to a PC.

****IMPORTANT****

Specify binary in your copy utility or ftp software when downloading the PROFBAS file to a PC. For all other files, specify fixed-length records and ASCII/text format. Basic ftp commands using a machine with sample IP address 193.241.02.85:

ftp 193.241.02.85 (establish an ftp connection with machine 193.241.02.85)

get sekchek/profbas *local_filename* (copy the *profbas* file from the remote machine to the default directory on the local machine. The *local_filename* in this case would be *Profbas.txt* in a specified directory on the PC)

bye (or **quit**) (exit ftp)

More information: <u>A sample ftp session</u>

7. Delete Temporary Files Created on AS/400

From the AS/400 command line enter:

RMVLIBLE SEKCHEK

DLTLIB LIB(SEKCHEK)

This will delete library SEKCHEK and its contents (i.e. all files/objects created during the Scan process).

Should you encounter difficulties with the process, <u>call us</u> with details of the problem and we will guide you through the process.

Next Step...

Encrypt the Scan Files on your PC

Encryption Instructions

Prerequisites

You should already have run the <u>Scan process</u>, which extracts files <u>PROFBAS</u>, <u>SYSVALS</u> & the (optional) files <u>ANZDFTPWD</u>, <u>PGMADP</u>, <u>SEKLOG</u>, <u>SRVTBLE</u> & <u>OBJAUT</u> from the AS/400 computer.

Outline of this Step





PROFBAS,SEKASF.ZIP/SYSVALSEncryptSEKASF.SCK

1. Encrypt the Scan Files

Copy files <u>PROFBAS.TXT</u>, <u>SYSVALS.TXT</u> and (if extracted) <u>ANZDFTPWD.TXT</u>, <u>OBJAUT.TXT</u>, IP/ <u>SEKLOG.TXT</u>, <u>SRVTBLE.TXT</u> & <u>PGMADP.TXT</u> to the desired directory on

your PC.

The encrypted file <u>SEKASF.ZIP</u> or <u>SEKASF.SCK</u> will be written to **the same directory**.

The downloaded files must have a .TXT file extension in order to be recognised by the Encryption Software.

Notes:

For enhanced security, we recommend that you enable *SekChek's* 'Public Key Encryption' features. For additional information, refer to <u>SekChek's Public Key Encryption</u>.

If 'Public Key Encryption' is enabled, *SekChek* will create an encrypted file named <u>SEKASF.SCK</u>. This file can only be decrypted with *SekChek*'s Private Key.

If 'Public Key Encryption' is not enabled, *SekChek* will create an encrypted file named <u>SEKASF.ZIP</u>.

AS/400 Netware UNIX Create Scan Software reate Scan software for execution on a OS/400 system Creat			
I. Create Scan Software Create Scan software for execution on a OS/400 system Creat	AS/400	Netware	UNIX
2. Run the Scan can security on a OS/400 (iSeries) system	. Create Scan Software - reate Scan software for . Run the Scan	ecution on a OS/400 system Series) system	Create

Select *Encrypt* in the *SekChek* for AS/400 application.

Follow the instructions on the screen... Select a valid Scan file (e.g. PROFBAS.TXT)...

Click *Encrypt*...

You will be prompted to enter basic information about your (client) organisation...

Click **OK**...

Next Step...

Send your Scan File for Processing

Sending your Scan File for Processing

Prerequisites

You should already have completed the following:

- Run the Scan process on the target system: <u>AS/400</u> system
 <u>Netware/Novell</u> system
 <u>Windows Server or Active Directory domain</u>
 <u>UNIX</u> system
- Encrypted the Scan files: <u>AS/400</u> system
 <u>Netware</u> system
 <u>UNIX</u> system
 <u>Windows</u> system

Outline of this Step



Send your Encrypted Scan File for Processing

 SEK??
 F.ZIP /
 Copy the encrypted Scan file

 SEK??
 inbox@sekchek.com
 (SEKASF.ZIP, SEKASF.SCK, SEKNEF.ZIP, SEKNEF.SCK, SEKNEF.ZIP, SEKNEF.SCK, SEKNTF.ZIP, SEKNTF.SCK, SEKNTF.ZIP, SEKNTF.SCK

<u>SEKUNF.ZIP</u>, <u>SEKUNF.SCK</u>, <u>SEK2KF.ZIP</u> or <u>SEK2KF.SCK</u>) to the desired directory on your PC.

Select *E-Mail* in the appropriate *SekChek* application.

Follow the instructions on the screen... Select the SEK??F.ZIP or SEK??F.SCK file... and add any special message to the standard text in the message box. The text that you insert here will be included in the body of a standard e-mail message addressed to *inbox@sekchek.com*.

Click *E-Mail*...

SekChek will prepare a formatted e-mail message containing your chosen SEK?? F.ZIP or SEK??F.SCK file as a file attachment and send it to your Outbox for onward transmission to us.

You can also send us the file by preparing a message with your e-mail client software (e.g. Outlook, cc:Mail) addressed to *inbox@sekchek.com*.

✓ Note:

SekChek will also recognise extended filenames (e.g. *SEKUNF MyHost.ZIP* and *SEK2KF MyName 20070316.SCK*) as long as the filename begins with one of

SekChek's 6 character prefixes (e.g. *SEKUNF*).

Notify Us if You do not Receive a Confirmation e-mail

We will e-mail an acknowledgement message to you within minutes of receiving your Scan file. Please advise us if you do not receive this acknowledgement.

Next Step...

SekChek Processing - An Overview

SekChek Processing

As soon as we receive your Scan file, we will:

- **Decrypt your file**, using the private key that resides at *SekChek*.
- **Send you a File Receipt** to let you know that your Scan file has arrived OK.
- **Process your Scan file**, using the latest version of the *SekChek* Processing Engine. The output report will be in MS-Word format.
- **Encrypt your report**, using the **password** that you chose when you ran the Scan process or encrypted the Scan file.
- **E-mail** your encrypted report package to your personal e-mail address.

We *guarantee* to despatch your encrypted report package within 24 hours of receiving your Scan file.

How Can You Contact Us?

Decryption Instructions

Prerequisites

You should already have completed the following:

- <u>Scanned</u> the AS/400 host and downloaded the Scan files (<u>PROFBAS.TXT</u> & <u>SYSVALS.TXT</u>);
- <u>Encrypted</u> these files and e-mailed them to us for processing;
- Received the file <u>SEKASR.SDE</u> from us. This file contains your encrypted *SekChek for AS/400* security report.

Outline of this Step



SEKASR.SDE Decrypt

Decrypt the *SekChek* **Report**

Copy file <u>SEKASR.SDE</u> to the desired directory on your PC. Note that your decrypted *SekChek* report will be written to **the same directory.**

Select the *SekChek* for AS/400 Tab, click *Decrypt*...

6. Decrypt report package	
Decrypt your encrypted SekChek report package	Decrypt

Follow the instructions on the screen... Ensure you select the correct report file, <u>SEKASR.SDE</u>. Click Decrypt...

Enter the same password you specified in the encryption process...

Click **OK**...

File <u>SEKASR.SDE</u> will be decrypted and your report written to file 'SekChek_AS400 Report xxxxx.doc'.

Clean-up

Once you are satisfied that the report is OK, you can delete file <u>SEKASR.SDE</u> if you wish.

Notes:

Passwords are case sensitive - I.e. 'seCret29' is different to 'secret29'.

The *Display File Header* option will display header information for any *SekChek* encrypted file. Encrypted File Headers contain information that can be used to uniquely identify *SekChek* files.

If you encounter problems, <u>phone or e-mail</u> us with details of the problem and we will help guide you through the process.
Overview





E-mail your encrypted *SekChek* report package (<u>SEKNER.SDE</u>) to you



SekChek Report



We provide you with:

- Detailed step-by-step instructions for all processes;
- Software to encrypt & decrypt the transmitted files.

Creating the Scan Software

The Scan software is used to scan security on a NetWare Server.

You can create a copy by clicking on the button *Create Scan software*.

View Options Tools H	Help	
AS/400	Netware	UNIX
1. Create Scan Software		\sim
Create Scan software for execut	ion on a Netware/Novell s	ystem Create

Next Step...

Scanning Security on a NetWare Server

Scan Instructions

Prerequisites

You should already have <u>created a copy of the Scan software</u> (SEKNEEXT.EXE).

Outline of this Step



Netware Server

Scan SEKNEF.ZIP

IMPORTANT

To ensure correct results use the ADMIN account for the following operations.

Running the Scan Software

1. Log into the Directory Tree (i.e. not a Server connection) from a Windows / NetWare Client machine as user 'Admin'

The requirements for running the *SekChek* Scan software are as follows:

• The user must be logged in the NDS tree from a workstation running the Novell Client Software

• For NT, 2000 and XP workstations it is recommended that you run *SekChek* on Novell Client version 4.70 or later

• For Windows 98 workstations it is recommended that you run *SekChek* on Novell Client version 3.20 or later

• To ensure the results are complete the software should be run under the Admin account.

2. Execute the Scan Software

Run program SEKNEEXT.EXE directly from the Scan software diskette or from a directory on a hard drive of the NetWare Client machine.

Follow the instructions on the screen... Select the Context you wish to analyse and the desired output directory - you can browse through the NDS Tree by clicking on the Browse Tree button.

3. Click 'Start Now' or 'Start Later'.

'Start Now' will execute the Scan process immediately.

'Start Later' will display a scheduler menu that allows you to select a specific time for SekChek to run, for example overnight or during a week-end. This is useful where the client is reluctant to run SekChek during prime business hours.

What the Scan software will do...

The software will scan security-related data in the chosen Context (default is [Root]). The data will be written to the encrypted file <u>SEKNEF.ZIP</u> in a directory of your choice.

Note that the software does NOT ADD TO, CHANGE, OR DELETE FROM the client's system in any way!

If you encounter difficulties with the process, <u>call us</u> with details of the problem and we will help guide you through the process.

Next Step...

Encrypt your Scan File

Encryption Instructions

Prerequisites

You should already have run the <u>Scan process</u> on the Netware system, which creates file <u>SEKNEF.ZIP</u>.

Outline of this Step

This step provides an additional layer of encryption for the Scan file created on the Netware system.



1. Encrypt the Scan file with Public Key Encryption

The Encrypt button will only be enabled if you selected SekChek's <u>Public Key</u> <u>Encryption</u> option (Tools / Options SEKNEF.SCK /General tab)

SEKNEF.ZIP Encrypt

Copy file <u>SEKNEF.ZIP</u> to the desired directory on your PC. Note that the output PKI-encrypted file <u>SEKNEF.SCK</u> will be written to **the same directory**.

Notes:

The downloaded files must have a .ZIP file extension in order to be recognised by the Encryption Software. The Public Key encrypted file, <u>SEKNEF.SCK</u>, can only be decrypted with *SekChek's* Private Key.

SekChek will also recognise extended filenames (e.g. *SEKNEF MyHost* 20070316.ZIP) as long as the filename begins with *SEKNEF*.

SekChek for NetWare	
ile View Options Tools Help	
AS/400 Netware	UNIX
1. Create Scan Software Create Scan software for execution on a Netware/Novell system	Create
2. Run the Scan Scan security on a Netware server	
- 3. Encrypt Scan file	Encrypt

Select *Encrypt* in the *SekChek* for Netware application in the *SekChek* Client Software.

Follow the instructions on the screen... Select the Scan file you want to encrypt...

Click *Encrypt*...

Next Step...

Send your Scan File for Processing

Decryption Instructions

Prerequisites

You should already have completed the following:

- <u>Scanned security</u> on the NetWare server
- <u>E-mailed</u> file <u>SEKNEF.ZIP</u> or <u>SEKNEF.SCK</u> to us for processing
- Received the file <u>SEKNER.SDE</u> from us. This file contains your encrypted *SekChek for Netware* security report

Outline of this Step



SEKNER.SDE Decrypt

Decrypt the SekChek Report

Copy file <u>SEKNER.SDE</u> to the desired directory on your PC. Note that your decrypted *SekChek for NetWare* report will be written to **the same directory**.

Select the *SekChek* for NetWare Tab, click *Decrypt*...



Follow the instructions on the screen... Ensure you select the correct report file, <u>SEKNER.SDE</u>. Click Decrypt...

Enter the same password you specified in the Scan process...

Click **OK**...

File <u>SEKNER.SDE</u> will be decrypted and your report written to file 'SekChek_NetWare Report xxxxx.doc'.

Clean-up

Once you are satisfied that the report is OK, you can delete file <u>SEKNER.SDE</u> if you wish.

Notes:

Passwords are case sensitive - I.e. 'seCret29' is different to 'secret29'.

The *Display File Header* option will display header information for any *SekChek* encrypted file. Encrypted File Headers contain information that can be used to uniquely identify *SekChek* files.

If you encounter problems, <u>phone or e-mail</u> us with details of the problem and we will help guide you through the process.

Overview



븹 (

E-mail your encrypted *SekChek* report package (<u>SEKWIR.SDE</u>) to you

SekChek Report



Decrypt your report

We provide you with:

- Detailed step-by-step instructions for all processes;
- Software to encrypt & decrypt the transmitted files.

Planning Your SekChek Analysis

For best results, before you use the *SekChek* Scan software, you should carefully consider which computers *SekChek* must run on to ensure that your particular objectives will be satisfied.

Ideally, this planning process requires some basic information about the client's computer network and a conceptual understanding of the function and relationships between standalone computers, domains, domain controllers and domain *trusts*.

Domains & Standalone Computers

Single Domain Model

Trust Relationships

Master Domain Model

Deciding Which Computers to Analyse

Domains & Standalone Computers

General:

Typically, Windows NT and Windows 200X computers (servers and workstations) are either free standing, within a workgroup, or are members of a domain.

A workgroup is a collection of Computers that are grouped together for the purpose of sharing resources. Each workgroup is identified by a unique name. Each computer in the workgroup has its own set of user accounts and groups that are independent of accounts defined on other computers. Workgroups do not have a centralised security database.

Windows NT:

In Windows NT, a domain is a collection of computers defined by the administrator of a Windows NT Server network that share a common directory/security database. A domain provides access to the centralized user accounts and group accounts maintained by the domain administrator. Each domain has a unique name.

Domain user accounts are defined on the Primary Domain Controller (PDC). Each account includes basic security information about the user and details of the account's group memberships etc. Although many security settings can be overridden at the user account level, accounts generally inherit security policy information (domain-wide security parameters) defined at the PDC level.

In addition to this central database of user accounts and groups for the domain, each server or workstation has its own local accounts database and groups. These are managed locally on each server or workstation.

One of the obvious considerations is that server and workstation security is dependent on a combination of security controls defined at the domain controller level and local security definitions.

Windows 2000/2003/2008

In Windows 2000/2003/2008, a domain is a collection of computers defined by the administrator of a Windows 2000/2003/2008 Server network that shares a common directory database (Active Directory).

Domain user accounts are defined on the Domain Controller(s) (DC). Each account includes security information about the user and details of the account's group memberships etc. Although many security settings can be overridden at the user account level, accounts generally inherit security policy information (domain-wide security parameters) defined at the DC level.

A domain provides access to the centralized user accounts and group accounts maintained by the domain administrator. Each domain defines both an administrative boundary and a security boundary for a collection of objects that are relevant to a specific group of users on a network.

A domain is an administrative boundary because administrative privileges do not extend to other domains. It is a security boundary because each domain has a security policy that extends to all accounts within the domain.

Domains can be organized into parent-child relationships to form a hierarchy, which is called a domain tree. The domains that are part of a domain tree implicitly trust each other. Multiple domain trees can be connected together into a forest. All trees in a given forest trust each other via transitive hierarchical trust relationships.

In addition to the central database of user accounts and groups for the domain, each server or workstation has its own local accounts database and groups. These are managed locally on each server or workstation.

Single Domain Model

This is a simple network configuration comprising one domain only.

An Active Directory domain consists of at least one Domain Controller (DC). Each DC contains a replica of the Active Directory database.



In a single domain network, network administrators can administer all servers connected to the domain, because security is centralised at the domain level. The single domain model is the building block for *all* multiple domain networks.

Trust Relationships

Trust relationships allow multiple domains to be logically connected and allow users to be authenticated on their primary domain, yet *gain access to resources connected to other domains without having to sign-on again to these other domains*. Using *Trust relationships* to connect domains, network designers can build extremely large and complex networks.

Trust relationships are easy to administer and facilitate:

- Centralised administration in multiple domain models.
- User logons from domains where they do not have accounts.
- Users from one domain to access resources in another domain, even if they do not have an account in that domain.
- Networks with larger numbers of users, by locating machine and resource accounts in other domains.



One- and Two-Way Trust Relationships

Trust relationships can be one- or two-way. The diagram above illustrates a oneway Trust relationship; Domain1 is trusting Domain2. I.e. All users from the trusted domain (Domain2) can access resources connected to the trusting domain (Domain1).

A two-way trust exists where both domains trust each other equally (see diagram below). Two-way trusts allow users defined in Domain1 and Domain2 to access resources connected to either domain.



One of the main considerations is that security on a *trusting* domain can be easily undermined by weak security standards and practices on a *trusted* domain.

Notes on Trust Relationships

A trust relationship is a link between two domains where the trusting domain honours logon authentications for the trusted domain.

Active Directory services support two forms of trust relationships: one-way, non-transitive trusts and two-way, transitive trusts.

In a one-way trust relationship, if Domain A trusts Domain B, Domain B does not automatically trust Domain A.

In a non-transitive trust relationship, if Domain A trusts Domain B and Domain B trusts Domain C, then Domain A does not automatically trust Domain C.

Networks running Windows NT 4.0 and earlier versions of Windows NT use one-way, non-transitive trust relationships. You manually create one-way, nontransitive trust relationships between existing domains. As a result, a Windows NT 4.0 (or earlier Windows NT) network with several domains requires the creation of many trust relationships.

Active Directory services support this type of trust for connections to existing Windows NT 4.0 and earlier domains and to allow the configuration of trust relationships with domains in other domain trees.

A two-way, transitive trust is the relationship between parent and child domains within a domain tree and between the top-level domains in a forest of domain trees. This is the default for Windows 200X. Trust relationships among domains in a tree are established and maintained automatically. Transitive trust is a feature of the Kerberos authentication protocol, which provides for distributed authentication and authorization in Windows 200X.

In a two-way trust relationship, if Domain A trusts Domain B, then Domain B trusts Domain A. In a transitive trust relationship, if Domain A trusts Domain B and Domain B trusts Domain C, then Domain A automatically trusts Domain C. Therefore in a two-way, transitive trust relationship, if Domain A trusts Domain B and Domain B trusts Domain C, then Domain A trusts Domain C and Domain C trusts Domain A.

If a two-way, transitive trust exists between two domains, you can assign permissions to resources in one domain to user and group accounts in the other domain, and vice versa.

Two-way, transitive trust relationships are the default in Windows 200X. When you create a new child domain in a domain tree, a trust relationship is established automatically with its parent domain, which imparts a trust relationship with every other domain in the tree. As a result, users in one domain can access resources to which they have been granted permission in all other domains in a tree.

Note, however, that the single logon enabled by trusts does not necessarily imply that the authenticated user has rights and permissions in all domains.

The trusting domain will rely on the trusted domain to verify the user accounts and passwords for users logging on the trusted domain.

Single Master Domain Model

The single master domain model is comprised of several domains, one of which acts as the central administrative unit for user accounts. User and machine accounts are defined in this *master* domain and all users log on to their accounts in the *master* domain.

Resources, such as printers and file servers, are located in the other domains (*resource* domains). Each *resource* domain establishes a one-way trust with the *master* (account) domain, enabling users with accounts in the master domain to use resources in all the other domains. The network administrator can manage the entire multi-domain network, including its users and resources, from a single domain.

This model balances the requirements for account security with the need to share resources via the network, because users are given permission to resources based on their master domain logon identity.

The single master domain model is particularly suited for:

- Centralised account management. Security and User accounts can be centrally managed from a single point.
- Decentralised resource management or local system administration capability. Department domains can have their own administrators, who manage the resources in the department.
- Resources can be grouped logically, corresponding to local domains.

Another type of domain model is the multiple master domain model, where different trust relationships can be implemented between master domains and resource domains within each master domain.

Active Directory domains offer more options where Resource Domains may not be necessary as they could for example, be implemented as Organizational Units.

Deciding which Computers to Analyse with SekChek

To ensure *SekChek* will provide you with the best results:

- Make sure you are clear on the scope of your review. E.g. do you want to analyse domain-wide security for one domain only, dial-in security (e.g. RAS) access to a domain, access to sensitive applications or data residing on specific servers or workstations, or enterprise-wide security on all *trusting* and *trusted* domains?
- Ensure you have a basic understanding of your client's computer network. If you are not certain, the quickest way to obtain this information is to run *SekChek* on a domain controller first.

This will provide you with analyses of all domain-wide security settings, all user accounts defined to that domain and details of all computers that are visible to the domain controller. It will also give you a summary of any Trust relationships that might exist with other domains on the network.

After you have studied the domain-wide security analysis, you might decide to run *SekChek* on a specific computer containing sensitive data or a particular application system, to obtain an analysis of security settings that are local to that computer.

An example would be a server running RAS software, which grants dial-in access (via a modem link) to remote users.

If *SekChek* is run on a domain controller, it will analyse those accounts with RAS access at domain level (only) and provide you with a list of all visible RAS servers. However, because accounts with RAS access can also be defined locally (i.e. on the RAS server itself), you would additionally need to run *SekChek* on each RAS server to obtain a complete picture of security controls over dial-in access.

If there are *trusted* domains, you should consider running *SekChek* on the

domain controllers for all *trusted* domains. This is because inappropriate security settings on *trusted* domains will threaten and undermine security on the *trusting* domain.

When planning your *SekChek* analyses, keep in mind that if *SekChek* is run on:

- A domain controller, it will report on security information at the domain level for users, accounts and groups and on domain-wide security (policy) settings.
- A server or workstation that is *not* a domain controller, it will report on security information at the local (server or workstation) level for users, accounts, groups and on security (policy) settings for that machine only. It will *not* analyse accounts and security settings defined at the domain level, although it will list any domain and workgroup memberships.

In summary, you will obtain the most comprehensive view of security by running *SekChek* on a combination of the *domain controller*, on *selected servers* containing sensitive data and systems, and on domain controllers for each *trusted* domain.

Creating the Scan Software

The Scan software is used to scan security settings and accounts on a Windows server (local security) or Active Directory domain (domain-wide security).

You can create a copy by clicking on the button *Create Scan software*..

SekChek for Windows File View Options Tool	s Help		
AS/400	Netware	UNIX	Windows
Create Scan Software	ecution on a Windows server or	domain Create	

Next Step...

Scanning Security on a Windows Server or Active Directory Domain

Scan Instructions

Prerequisites

You should already have <u>created a copy of the Scan software</u> (SEKWIEXT.EXE).

Outline of this Step



Scan

Windows NT/200X Server

SEKNTF.ZIP/ SEK2KF.ZIP

****IMPORTANT****

- 1. To ensure correct results use the Administrator account for the following operations.
- 2. The Scan process must be run on the computer (DC or Server) you want to analyse. Logon to the Server locally. See '<u>Planning your</u>

SekChek analysis' / '<u>Deciding which computers to analyse</u>' for more information.

- We recommend that you do not select the Windows System drive, or a low capacity removable drive, for *SekChek's* output files; they can extend to tens of megabytes in size.
- Note that the software does not add to or change the Host system in any way.

Running the Scan Software

1. Decide whether you want to analyse any special registry keys or DACLs on directories.

If you want to scan special registry keys or DACLs / SACLs defined on directories, you must define your requirements in a file named sekchek.inp. For details of how to do this see: www.sekchek.com/sekchek-windows-sekchekinp-

file.htm.

You can ignore this step if you do not want to scan registry keys and directory permissions.

2. Start the Scan software.

Run program SEKWIEXT.EXE on the NT or Windows 200X server from a directory on the network (preferred).

Windows 2008 systems: Right-click the Scan software (SEKWIEXT.EXE) and select 'Run as administrator'.



3. Select the path for SekChek output file.

Click 'Next'... 'Change Directory'...

4. Check / enter your processing options

Client Details The name of your organisation:		Evaluation Options
MyOrganisation		Standards template nbr: 0
Country where the Host is located:	Industry type:	Compare security against:
Spain 💌	Hotels and Catering	Hotels and Catering 🗨
Charge (DIS) code:		Compare Against Previous RefNbr:
My Internal Code		
Scan Organizational Unit (OU) objects	s for DACLs	
Scan Organizational Unit (OU) objects	s for DACLs	
Scan Organizational Unit (OU) objects iew / Change Options Client & run-time options	s for DACLs	

5. Click 'Start Now' or 'Start Later'

'Start Now' will execute the Scan process immediately. SekChek will display the progress of the Scan.

'Start Later' will display a scheduler menu that allows you to select a more convenient time for SekChek to run. This is useful if you want to run SekChek outside prime business hours.

To Scan Last Logon Information from all Domain Controllers in a Windows Domain (Optional step)

Window's domains do not replicate account's last logon information across domain controllers. Each Domain Controller, within the domain, stores the details of the last logon information for accounts that the controller authenticated to the domain.

The *SekChek* for Windows Scan Software includes an optional check-box, '*Query all DCs for Last Logon details*', that allows a user to retrieve all last logon information stored on Domain Controllers. When the '*Query all DCs for Last Logon details*' check-box is enabled, the *SekChek* for Windows software will attempt to access all visible domain controllers on the network and retrieve last logon details from each domain controller.

✓ Notes:

The'**Query all DCs for Last Logon details**' check-box is only available when the *SekChek* for Windows Scan Software is run on a Domain Controller. This option will not be available when the Scan process is run on stand-alone servers or workstations.

If domain controllers exist in a separate physical location from the domain controller where the Scan software is run, the time required for the Scan process to complete can increase significantly.

If the *SekChek* for Windows Scan software is initiated with the '*Query all DCs for Last Logon details*' check-box unchecked, only the last logon information for the local domain controller will be retrieved.

What the Scan software will do...

The software will scan security-related data on the Windows system and write it to an encrypted file <u>(SEKNTF.ZIP</u> or <u>SEK2KF.ZIP</u>) in a directory of your choice.

We do not recommend that you write the file to a diskette as it could exceed the diskette's storage capacity.

Next Step...

Encrypt the Scan File on your PC

Encryption Instructions

Prerequisites

You should already have run the <u>Scan process</u> on the Windows server or Active Directory domain, which creates file <u>SEKNTF.ZIP</u> or <u>SEK2KF.ZIP</u>.

Outline of this Step

This step provides an additional layer of encryption of the Scan file.





1. Encrypt the Scan file with Public Key Encryption

The Encrypt button will only be enabled if you selected SekChek's <u>Public Key</u> <u>Encryption</u> option (Tools / Options /

SEKNTF.ZIP or Encrypt SEK2KF.ZIP SEK2KF.ZIP SEK2KF.ZIP (or SEK2KF.SCK Copy file SEK2KF.ZIP (or SEKNTF.ZIP) to the desired directory on your PC. Note that the output PKI-encrypted file (SEKNTF.SCK or

<u>SEK2KF.SCK</u>) will be written to **the same directory**.

Notes:

The downloaded files must have a .ZIP file extension in order to be recognised by the Encryption Software. The Public Key encrypted file, <u>SEKNTF.SCK</u> or <u>SEK2KF.SCK</u>, can only be decrypted with *SekChek's* Private Key.

SekChek will also recognise extended filenames (e.g. *SEKNTF MyHost.ZIP* and *SEK2KF MyName 20070316.ZIP*) as long as the filename begins with *SEKNTF* or *SEK2KF*.

A Sy400 Netware ONDA	AC/400	Notwara		Windows
1. Create Scan Software Create Scan software for execution on a Windows server or domain 2. Run the Scan Scan security on a Windows server or domain 3. Encrypt Scan file	A5/400	Netware	VINIX	windows
Create Scan software for execution on a Windows server or domain Create	1. Crasta Com Coffuero			
Create Scan software for execution on a Windows server or domain 2. Run the Scan 3. Encrypt Scan file	- 1. Create Scan Software			
2. Run the Scan Scan security on a Windows server or domain 3. Encrypt Scan file	Create Scan software for e	xecution on a Windows server or	domain Create	
2. Run the Scan Scan security on a Windows server or domain 3. Encrypt Scan file				
-2. Run the Scan Scan security on a Windows server or domain -3. Encrypt Scan file				
Scan security on a Windows server or domain 3. Encrypt Scan file	0.0.11.0			
-3. Encrypt Scan file	-2. Run the Scan			
- 3. Encrypt Scan file	 Run the Scan Scan security on a Windows 	server or domain		
-3. Encrypt Scan file	- 2. Run the Scan Scan security on a Windows	server or domain		
	- 2. Run the Scan	server or domain		
Encrypt Scan files using Public Key Encryption	2. Run the Scan Scan security on a Windows 3. Encrypt Scan file	server or domain		

Select *Encrypt* in the *SekChek* for Windows application in the SekChek Client Software.

Follow the instructions on the screen... Select the Scan file you want to encrypt...

Click *Encrypt*...

Next Step...

Send your Scan File for Processing

Decryption Instructions

Prerequisites

You should already have completed the following:

- <u>Scanned</u> security on the NT or Windows 2000 & later server
- <u>E-mailed</u> file <u>SEKNTF.ZIP/SEKNTF.SCK</u> or <u>SEK2KF.ZIP/SEK2KF.SCK</u> to us for processing
- Received the file <u>SEKWIR.SDE</u> from us. This file contains your encrypted *SekChek for Windows* security report

Outline of this Step



Decrypt the SekChek Report

Copy file <u>SEKWIR.SDE</u> to the desired directory on your PC. Note that your decrypted *SekChek* for Windows report will be written to **the same directory.**

Select the SekChek for Windows Tab, click Decrypt...



Follow the instructions on the screen... Ensure you select the correct report file, <u>SEKWIR.SDE</u>. Click Decrypt...

Enter the same password you specified in the Scan process...

Click **OK**...

File <u>SEKWIR.SDE</u> will be decrypted and your report written to file 'SekChek_NT Report xxxxx.doc' or 'SekChek_Win2000 Report xxxxx.doc'.

Clean-up

Once you are satisfied that the report is OK, you can delete file <u>SEKWIR.SDE</u> if you wish.

Notes:

Passwords are case sensitive - I.e. 'seCret29' is different to 'secret29'.

The *Display File Header* option will display header information for any *SekChek* encrypted file. Encrypted File Headers contain information that can be used to uniquely identify *SekChek* files.

If you encounter problems, <u>phone or e-mail</u> us with details of the problem and we will help guide you through the process.
Overview



Create the Scan Software

Ĵ

UNIX Host

Run the Scan process, download the Scan file to a PC

Ĵ

Ellin



Scan Files: <u>sekunf.z</u> or 25-30 text files (dependent on the availability of certain software on the host)



Encrypt the extracted security data in SEKUNF.ZIP E-mail the encrypted files for processing



SekChek Premises



Decrypt the SEKUNF.ZIP or SEKUNF.SCK file and produce your SekChek Report

Ĵ



E-mail your encrypted *SekChek* report package (<u>SEKUNR.SDE</u>) to you

Ĵ

SekChek Report



We provide you with:

- Detailed step-by-step instructions for all processes;
- Software to encrypt & decrypt the transmitted files.

Creating the Scan Software

The Scan software is used to scan security accounts and settings on a UNIX machine.

You can create a copy by clicking on the button *Create Scan software*.

SekChek for UNIX		
File View Options Tools	Help	
AS/400	Netware	
1. Create Scan Software Create Scan software for exe (any variant that supports the	cution on a UNIX system Bourne shell)	Create
2. Run the Scan		

Next Step...

Scanning Security on a UNIX System

Scan Instructions

Prerequisites

You should already have <u>created a copy of the Scan software</u> (SEKUNEXT).

Outline of this Step



UNIX Host Scan File(s)

****IMPORTANT****

- 1. To ensure correct results use the root account for the following operations
- 2. SekChek for UNIX will run on any system that supports the Bourne shell
- 3. Other than the security scan data written to sub-directory sekchek/ (see below), the Scan process does NOT ADD TO, CHANGE, OR DELETE FROM the client's system in any way!

Running the Scan Software

1. Copy the Scan Software to a Directory on the UNIX Machine

Copy file SEKUNEXT from diskette to a directory on the UNIX machine

Important! Specify binary (i.e. not ASCII) in your copy utility or ftp software to ensure that CR/LF characters are properly converted.

See <u>below</u> for examples of basic ftp commands.

2. Ensure the ROOT account has Authority to Execute the Scan Software

From the shell prompt enter: **chmod 700** /**tmp**/**SEKUNEXT** (where *tmp* is the

full name of the directory containing *SEKUNEXT*)

3. Change your Working Directory to the Desired Output Directory

From the shell prompt enter: **cd** /**tmp** (where *tmp* is the full name of the directory to contain *SekChek's* output files)

SekChek will automatically create a sub-directory (in Step 4 below) called '*sekchek*' in your (current) working directory and write it's Scan files to it. E.g. if your current working directory is '*/tmp*', your scan files will be written to directory '*/tmp/sekchek/*'.

You should ensure the partition has 20Mb of free space for *SekChek's* output files.

4. Execute the Scan Software

From the shell prompt enter: **sh** (to ensure you are in the Bourne shell)

Then enter: **/tmp/SEKUNEXT** (where *tmp* is the full name of the directory containing *SEKUNEXT*)

The software will ask if you want to scan details of:

- Programs that Switch User Id (SUID)
- Permissions on programs in the system search path
- Files with world writeable permissions
- Encrypted password information
- Permissions on files stored on NFS mounted volumes

If you are *not* interested in this information we recommend you reply 'N'. This is because on systems with large file systems it can take several hours to scan this data.

See <u>below</u> for an explanation of these run-time options, including their impact on your *SekChek* report.

SekChek will scan security data on the UNIX host and write it to sub-directory

'*sekchek*' in your (current) working directory. It will either create *one* file (<u>sekunf.z</u>) only, or 20-30 text (.txt) files, depending on the availability of certain software on the machine.

5. Copy the Scan File(s) to Diskette & Clean-Up

After the Scan Software has completed, you will need to:

- Copy the file(s) in directory */pathname/sekchek/* to diskette. *Ensure you specify 'binary'* (i.e. not ASCII or TXT) format in the copy/ftp operation.
- Delete all files in directory /pathname/sekchek/ (e.g. **rm** /**tmp**/**sekchek**/*). Make certain you enter this command correctly, otherwise you risk deleting many other files also!
- Remove sub-directory /sekchek (e.g. rmdir /tmp/sekchek)

Basic ftp Commands.

ftp 193.241.02.85 (establish an ftp connection with machine 193.241.02.85)

cd /tmp (change the default directory on the remote machine to e.g. /tmp)

binary (change FTP's transfer mode to binary)

get remote_filename [local_filename] (copy remote_filename from the default directory on the remote machine to the default directory on the local machine)

put local_filename [remote_filename] (copy local_filename from the default directory on the local machine to the default directory on the remote machine)

bye (or **quit**) (exit ftp)

Values inside square brackets [] are optional.

Sample command to create a sub-directory on the UNIX machine (optional). From the shell prompt on the UNIX machine, enter:

mkdir /tmp/mydir

(This command will create a sub-directory called 'mydir' in directory '/tmp')

More information: <u>A sample ftp session</u>

Run-time Options.

Programs that Switch User Id (SUID)

- These programs assume the identity of the user owning the executable [often root], rather than the user executing the program. It is important to maintain strong permissions on these programs because unauthorised changes [or program substitutions] could allow intruders to gain access to the root account and to all resources on your system.
- If you choose not to scan these permissions, your *SekChek* report will not contain information on programs that SUID.

Permissions on programs in the system search path

- This step will scan permissions on all files residing in all directories in the system search path. This path is searched each time a program or command is executed to determine the location of the program. Inappropriate permissions on these programs could lead to unauthorised changes [or program substitutions], which could have serious security implications.
- If you choose not to scan these permissions, your *SekChek* report will not contain information on programs in the System Path.

Files with world writeable permissions

- This step will scan a list of all files with world-writeable permissions on them. World-writeable permissions on a program or file allow ALL users with access to your system to change or delete the file. Sensitive files or programs should not be world-writeable and should be assigned to an appropriate owner.
- If you choose not to scan this list, your *SekChek* report will not contain information on files with world-writeable permissions.

Encrypted password information

- This step will scan encrypted password information in password and shadow password files. This will allow *SekChek* to analyse password triviality and determine which accounts are disabled.
- If you choose not to scan encrypted password information, the encrypted passwords will be replaced with "USER_WITHHELD" in SekChek's Scan file.
- Note that encrypted password information on Trusted Computer Based systems that store data in non-text format will not be replaced with "USER_WITHHELD" and will therefore be written to the Scan file.
- If you choose not to scan encrypted password information, your *SekChek* report will not contain analyses of trivial passwords or disabled user accounts.

Permissions on files stored on NFS mounted volumes

- This step will include NFS mounts in the Scan of file and directory permissions. NFS (Network File System) mounts are links to directories residing on remote servers.
- If you choose not to scan permissions on files in NFS Mounts, your *SekChek* report will only analyse permissions on files and directories residing on local disks.

Write Host details to a header in the Scan File

This option will write the Host name and Username to a clear text header in the Scan file. This can be useful for identification purposes.

If you encounter difficulties with the process, <u>call us</u> with details of the problem and we will guide you through the process.

Next Step...

Encrypt the Scan File (on your PC)

Encryption Instructions

Prerequisites

You should already have <u>run the Scan process</u> on the UNIX host system.

Outline of this Step



Scan Files

1. Encrypt the Scan File(s)

Copy the Scan file(s) to an *empty* directory on your PC. The number of Scan files could be one only (<u>sekunf.z</u>)

Encrypt SEKUNF.ZIP/ or 20-25 text files (refer note in the Scan SEKUNF.SCK Instructions).

The encrypted file <u>SEKUNF.ZIP</u> or <u>SEKUNF.SCK</u> will be written to **the same directory**.

Notes:

For enhanced security, we recommend that you enable *SekChek's* 'Public Key Encryption' features. For additional information, refer to <u>SekChek's Public Key Encryption</u>.

If 'Public Key Encryption' is enabled, *SekChek* will create an encrypted file named <u>SEKUNF.SCK</u>. This file can only be decrypted with *SekChek*'s Private Key.

If 'Public Key Encryption' is not enabled, *SekChek* will create an encrypted file named <u>SEKUNF.ZIP</u>.

SekChek will also recognise extended filenames (e.g. *SEKUNF MyHost 20070316.Z*) as long as the filename begins with *SEKUNF*.

i a la ca		
AS/400	Netware	UNIX
L. Create Scan Software		
Create Scan software for execu	tion on a UNIX system	Create
any variant that supports the E	Bourne shell)	Create
2. Run the Scan		
can security on a UNIV system		
scan security on a ONLX system		
3. Encrypt Scan file		

Select *Encrypt* in the *SekChek for UNIX* application.

Follow the instructions on the screen... Select the Scan file you want to encrypt...

Click *Encrypt*...

You will be prompted to enter basic information about your (client) organisation and your secret password that will be used to encrypt the report that is sent back to you.

Click **OK**...

We strongly recommend that, for enhanced high security, the *SekChek* Public/Private Key Encryption option is used. For additional information, refer to <u>SekChek's Public Key Encryption</u>.

Next Step...

Send your Scan File for Processing

Decryption Instructions

Prerequisites

You should already have completed the following:

- <u>Scanned</u> security data on the UNIX host
- <u>E-mailed</u> file <u>SEKUNF.ZIP</u> or <u>SEKUNF.SCK</u> to us for processing
- Received the file <u>SEKUNR.SDE</u> from us. This file contains your encrypted *SekChek for UNIX* security report

Outline of this Step



Decrypt the SekChek Report

Copy file <u>SEKUNR.SDE</u> to the desired directory on your PC. Note that your decrypted *SekChek for UNIX* report will be written to **the same directory.**

Select the *SekChek* for UNIX Tab, click *Decrypt*...

6. Decrypt report package	
Decrypt your encrypted SekChek report package	Decrypt

Follow the instructions on the screen... Ensure you select the correct report file, <u>SEKUNR.SDE</u>. Click Decrypt...

Enter the same password you specified in the encryption process...

Click **OK**...

File <u>SEKUNR.SDE</u> will be decrypted and your report written to file 'SekChek_UNIX Report xxxxx.doc'.

Clean-up

Once you are satisfied that the report is OK, you can delete file <u>SEKUNR.SDE</u> if you wish.

Notes:

Passwords are case sensitive - I.e. 'seCret29' is different to 'secret29'.

The *Display File Header* option will display header information for any *SekChek* encrypted file. Encrypted File Headers contain information that can be used to uniquely identify *SekChek* files.

If you encounter problems, <u>phone or e-mail</u> us with details of the problem and we will help guide you through the process.

The Utilities Screen

The Purpose of this Screen

This Utilities screen provides access to tools that automate commonly performed tasks.

AS/400	Netware	UNIX	Windows	Utilities
ervice Request Utility: Send e-r	mail to SekChek to request			
Decryption passwords	Status of report processing	Letter of assu	rance	
Latest SekChek software	Marketing brochure	🔲 SekChek's digi	tal certificate	
SekChek newsletter	Assistance (send log file)	Your customer	code	Send <u>R</u> equest
le Splitter Utility		SekCrypt General	Purpose Symmetric Encryption	Utility
File Splitter Utility		SekCrypt General	Purpose Symmetric Encryption	Utility

Service Request Utility

Generates automated Service Requests, which are sent to *SekChek's* email address at <u>inbox@sekchek.com</u>. The items you request will be automatically despatched to your e-mail address.

- Decryption passwords: Requests the passwords used to encrypt the last 15 *SekChek* reports submitted for processing from your email address.
- Status of Report processing: Requests the status for your previous 10 analyses submitted for processing from your email address.
- SekChek's Letter of Assurance:
 Letter of Assurance regarding the impact of SekChek on a Host computer;
 SekChek's standards and procedures for ensuring confidentiality over client data.
- Latest *SekChek* software: Requests a copy of the latest version of the Client software.

- *SekChek* Marketing Brochure: Requests a copy of our electronic marketing brochure.
- *SekChek's* digital certificate: Requests a copy of our Digital Certificate used for the Public Key encryption of Scan data.
- SekChek Newsletter: Requests a copy of our latest Newsletter.
- Assistance (send log): Requests assistance from *SekChek* and attaches a copy of *SekChek's* logfile.
- Your Customer Code: Requests your customer account code, against which *SekChek* services are charged. It is listed on the first page of your SekChek report.

File Splitter Utility

This utility will split any large file into a collection of smaller files. You can control the size of the output files, in bytes, in the range 10,000 (10KB) to 10,000,000 (10MB).

Smaller files can speed up the transmission process and allow you to bypass any file size restrictions that may exist on your firewall. A general recommendation is that you should consider splitting Scan files larger than 5MB into several smaller files of 2MB (2,000,000) each.

To join a file that has been split using the *SekChek* File Splitter Utility, select one of the split-file collection... Click Join.

☑ Note:

When joining split-files, ensure that the full collection of split-files is present in the same directory.

SekCrypt Encryption/Decryption Utility

SekCrypt is a general purpose symmetric encryption tool that allows you to encrypt / decrypt any file using industry-standard encryption algorithms, such as AES (Rijndael), and DES.

After you have selected a file to encrypt or decrypt you will be prompted to enter a secret pass-phrase. The output encrypted (or decrypted) file will be created in the same directory as the input file. Decrypted files will have the same filename as the original, encrypted file. SekCrypt will issue a prompt to overwrite if a file with the same name already exists.

All files created by SekCrypt or the *SekChek* Client software contain a special <u>Encrypted File Header (EFH)</u>. Click on the link for more information.

✓ Notes:

Files encrypted by SekCrypt always have a .SDE file extension. The Decrypt function will not recognise files with any other extension.

When encrypting files, SekCrypt will use the 3DES algorithm by default. However, you can override this by checking the 'Enforce Algorithm' checkbox and selecting the algorithm of your choice from the drop-down listbox.

When decrypting SDE files, SekCrypt will automatically try to locate the same algorithm that was used to encrypt the file. It will issue an error message if the required algorithm is not installed on your system. It is possible that the relatively recent AES algorithm (in particular) may not exist on some older systems.

Pass-phrases are case-sensitive. If you forget your pass-phrase, you will not be able to decrypt your file!

File Drag / Drop Support

Note that the File Splitter and SekCrypt utilities provide support for <u>dragging /</u> <u>dropping</u> files. Try this out by dropping a file into one of the utility boxes.

SekChek's Public Key Encryption

What is Public Key Encryption?

Public Key Encryption (PKI) is an encryption technique that uses a pair of keys to encrypt and decrypt data. A key pair consists of a Public key and a Private key that are created to work together.

The Public key is typically distributed at large and the Private key is held only by a single party. When data is encrypted with the Public key, the data can only be decrypted by the holder of the corresponding Private key.

One of the main differences between Public Key Encryption techniques and traditional, Symmetric Encryption techniques is that Public Key Encryption does not require a secret key (password) to be exchanged between the encrypting and decrypting parties.

SekChek Uses X.509 Digital Certificates

SekChek stores its Public key in an industry-standard X.509 digital certificate. This means that certificates shipped with the *SekChek* Client software are fully compatible with Microsoft's security interfaces and certificate management wizards. X.509 certificates also integrate seamlessly with products such as Internet Explorer and Microsoft Outlook.

Why should I use SekChek's Public Key Encryption Features?

SekChek's public key encryption features provide several advantages over symmetric encryption techniques:

Your data is more secure. This is because *SekChek* uses robust, industry-standard encryption algorithms, such as RSA and 3-DES.

You do not have to transmit a secret password to us. This saves you valuable time. It also reduces the turnaround time for your *SekChek* reports because we do

not have to contact you for the password that was used to encrypt your Scan file. Another benefit is that it eliminates the need to re-encrypt a file or rerun the Scan program if the encryption password was mistyped or has been forgotten.

The really good news is that the process is almost totally transparent. All you need do, to ensure public key encryption is used for all your Scan files, is to enable (click-on) the 'Public Key Encryption' checkbox in the Client software ('Options' screen).

The Client software is also used to encrypt your Scan files from Windows and Netware systems to *SekChek's* public key.

Although we recommend that you use *SekChek's* Public Key Encryption (high security) features, these features are optional. If you choose not to use *SekChek's* Public Key Encryption, *SekChek* will encrypt your Scan files with a modified proprietary encryption algorithm that does not require a password.

How do I enable the Public Key Encryption features?

- 1. Go to Options | User Preferences
- 2. Select (check) the 'Use Public Key Encryption' checkbox

How are SekChek's Reports encrypted?

Regardless of which encryption technique you select when encrypting the Scan file, your *SekChek* report will always be encrypted using an industry-standard password-based (symmetric) encryption algorithm.

The password required to decrypt your report must be the same as the password you entered when encrypting the Scan file.

SekChek's Certificate

To ensure the authenticity of the Certificate, please check that it has the following properties:

NameSekChek Information ProtectionServices CC

Serial Number	5c c0 4c b3 82 16 1d 39 7a 85 a3 9d ac 0c fb 91
Thumbprint (sha1) 2f e7 7a	13 3a 91 ef ed 3b 2a 04 65 06 51 9f db 40 e5 15 06

If the Certificate's Serial Number or Thumbprint are different to the above values, please cancel the installation and contact *SekChek* for assistance.

Refer to our <u>CPS</u> (Certification Practice Statement) for details of controls over SekChek's private keys or <u>write to us</u> for more information regarding Public Key encryption.

SekChek's Naming Conventions for Encrypted Files

SekChek employs various industry-standard encryption algorithms and techniques to ensure the security of your data. These include Public Key encryption techniques based on the RSA algorithm, and symmetric encryption techniques using algorithms such as AES, DES and 3DES as well as proprietary methods.

The extensions of files encrypted by *SekChek* reflect the type of encryption they were created with and can be any of the following:

- .ZIP
- .SCK
- .SDE

.ZIP Files

A ZIP file extension indicates that the file was encrypted using *SekChek's* proprietary encryption techniques.

ZIP files are always created by the *SekChek* for Windows and Netware Scan software that runs on the target system. We recommend that these files are additionally encrypted with *SekChek's* Public key. You can do this via the Client software on your PC after turning on (checking) the 'Public Key Encryption' option. The process will create a file with an SCK extension. This is the file that should be sent to *SekChek* for processing.

ZIP files are also created by the Client software when you encrypt Scan files from an AS/400 or UNIX system with the 'Public Key Encryption' option turned off (unchecked). For additional security, we recommend that you always encrypt Scan files with the 'Public Key Encryption' option turned on (checked). The process will create a file with an SCK extension. See below for an explanation of the encryption methods used to create an SCK file.

.SCK Files

A SCK file extension indicates that the Scan file was encrypted with *SekChek's* Public Key using industry-standard encryption algorithms, such as RSA and 3-DES. SCK files can only be decrypted with *SekChek's* non-exportable Private Key, which can only be accessed under controlled conditions at our secure premises.

SCK files are created by the Client software when the 'Public Key Encryption' option is enabled (checked). The feature is located on the 'Options' page of the *SekChek* Client Software. We recommend that you enable this option to ensure all of your *SekChek* files are protected by state-of-the-art encryption techniques.

.SDE Files

A SDE file extension indicates that the file was symmetrically encrypted using industry-standard algorithms, such as AES (Rijndael), 3DES and DES. SDE files typically contain *SekChek* reports.

If you would like to know more about *SekChek's* naming conventions for encrypted files, please <u>contact</u> us for more information.

For additional information on *SekChek's* encryption techniques, refer to <u>SekChek's Public Key Encryption</u>.

SekChek and Compliance Reviews (e.g. SOX)

The Sarbanes-Oxley legislation requires that companies assess the effectiveness of security controls at a point-in-time and on an ongoing basis.

SekChek is the ideal tool to analyse operating systems security controls on a frequent (e.g. quarterly) basis for period-on-period comparison.

The benefits of using *SekChek* as part of a SOX or other compliance review are:

- An *independent* point-in-time snapshot of security controls;
- The graphical analyses provide a quick indication of whether security controls have *strengthened* or *weakened* since the previous time *SekChek* was run on a platform;
- *Consistent* reporting from one analysis to the next avoids the risk of inconsistent interpretations between analyses over time;
- Similar reporting formats across platforms analysed (Windows, UNIX, AS400 and NetWare) ensure a *consistent* standard in the interpretation of security controls.



A collection of easy-to-read reports in a very familiar format provides you with visual indicators of:

- Whether security has improved, weakened, or remained about the same since your previous analysis
- The effectiveness of your measures to strengthen controls
- Whether risk is increasing or decreasing
- The degree of change, both positive and negative

The applications are endless. Some of the practical benefits are:

- Time savings. Reduced time spent poring over volumes of unconnected information
- Objectivity. The results are guaranteed to be the same regardless of who performs the review
- Compliance with legislation. Easier monitoring for compliance with statutory requirements imposed by SOX, HIPAA and other legislative changes relating to corporate governance
- More powerful justifications. The ability to present more convincing arguments to senior, non-technical management who do not have the time, or the inclination, to understand masses of technical detail

For additional information refer to <u>Requesting Time-Comparative Analyses</u> <u>Graphs</u>.

SekChek® is a registered trademark of SekChek IPS. All other trademarks are the property of their respective owners.

How Do I Request a Time-Comparative Analysis?

You simply need to supply us with the <u>Reference Number</u> for the previous analysis of the system. You will find the <u>Reference Number</u> on the first page of your *SekChek* report.

You can enter the previous <u>Reference Number</u> during the dialogue that is displayed for:

- Windows and Netware during the Scan process;
- AS/400 and UNIX during the encryption process in the Client software.

Client Details The name of your (or your dient's) orga	nisation:	Evaluation Options
MyOrganisation		Standards Template Nbr:
Country where the Host is located:	Industry type:	Compare security against:
Democratic Republic of Congo	Engineering	Engineering
Charge (DIS) code:		Compare Against Previous RefNbr:
My Internal Code		960 10 1000 1
Notes		
These values will be embedded in the Sc on the host system.	an software. They will be displaye	ed as default (initial) values during the Scan process
Note that these defaults can be change	d at execution time. The final valu	ies are embedded in the encrypted output file.
	antions during the Compression	on the heat sustam

Alternatively, you can simply include your request in the email to <u>inbox@sekchek.com</u> that contains your Scan file. Remember to include the <u>Reference Number</u> for the previous analysis!

Contact us for more information.

SekChek Local & Mobile-SekChek

What is SekChek Local?

SekChek Local scans security on one or more target systems from a workstation connected to your network. Scan data is processed entirely on your workstation, so there is no requirement to send data off-site for evaluation and processing, and minimal impact on the target systems or domain. There are no licensing requirements for the tool, so you can use it on a 'pay-as-you-go' basis.

SekChek Local provides you with:

- A Report Database in MS-Access format containing a comprehensive collection of summary and detailed reports.
- Access to powerful data manipulation and query utilities, which means you can develop your own customised queries.
- Fast turnaround time. Reports are typically available within minutes of completing a Scan.

<u>Click here</u> to download the software, sample reports or detailed technical specification documents. <u>Write to us</u> if you would like to request a no obligation free trial.

What is Mobile-SekChek?

The Mobile-*SekChek* service is designed for situations where policy prevents *SekChek* files from being sent outside organisational boundaries for reasons of security or confidentiality. It is a very personal and confidential service.

A senior consultant will travel to your - or your client's - premises with the *SekChek* Processing Engines installed on a high-powered laptop computer. *SekChek* files are processed on-site and Client data is deleted from the laptop after the Scan files have been processed. The consultant will summarise and

discuss the analyses and reports with you and your client.

What if I forget my password?

If you forget the password that was used to encrypt your report, don't worry.

You can obtain a list of all your recent passwords via SekChek's <u>Service Request</u> <u>system</u>. Our automated Request Handling system is available on a 365 x 24 hour basis, so you will receive a response within minutes of your request being received.

If you have a digital certificate and you are interested in receiving Report packages encrypted with your public key, send us a copy of your certificate (as a .CER file) and request that we use <u>PKI encryption</u> techniques, rather than password-based encryption techniques, to secure your SekChek Reports.

Why are *SekChek's* ZIP files being stripped from my emails?

The most likely reason is that your anti-virus software or firewall machine is configured to quarantine or strip all encrypted ZIP files.

The recommended solution is to encrypt your Scan file using *SekChek's* <u>Public/Private Key</u> encryption option. This will generate an SCK file that will pass through your firewall without interference.

You can turn on this option by enabling the <u>'Use Public Key Encryption</u>' checkbox on the Options Menu.

Why can't the Encrypt function 'see' my Scan files?

The most likely reason is that your Scan file is incorrectly named.

For example:

- SekChek for AS/400: The files must have '.txt' extensions, such as PROFBAS.TXT, SYSVALS.TXT.
- SekChek for UNIX: The file must be named sekunf.z or sekunf.tar. In certain cases you may have a collection of '.txt' files, such as hostname.txt etc.
- SekChek for Windows: The file must be named SEK2KF.ZIP or SEKNTF.ZIP. The Encrypt function will also recognize files with extended names, such as 'SEK2KF MyDescription.zip'. However, it will not recognize file 'MyDescription SEK2KF.ZIP'.
- SekChek for Netware: The file must be named SEKNEF.ZIP. The Encrypt function will also recognize files with extended names, such as 'SEKNEF MyDescription.ZIP'.

See <u>Encrypting your Scan File</u> for more information.

Why can't I decrypt my SekChek report with WINZIP?

The *SekChek* software uses a special algorithm to ensure your files are securely encrypted during transmission. This means you must have the *SekChek* software *and* know the private password to decrypt an encrypted file.

SekChek® is a registered trademark of SekChek IPS. All other trademarks are the property of their respective owners.

Error 'NTVDM encountered a hard error.' when executing the Windows Scan software.

When you attempt to execute the SekChek for Windows Scan software (SEKWIEXT.EXE) a warning message box is displayed with the title 'ntvdm.exe - System Error' and text 'NTVDM encountered a hard error.', reply Close or Ignore.

The error occurs because file SEKWIEXT.EXE is corrupt. This is often caused by anti-virus software.

The solution is to obtain a fresh copy of SEKWIEXT.EXE or to create it via the SekChek Client software, which is located on our web site. The size of file SEKWIEXT.EXE is about 1.4 MB.

Why do I receive the message "SekChek's digital certificate is expired or damaged" when I try to enable the PKI features?

It is possible that the certificate has expired.

However, the most likely reason is that your system's policies prevent third-party Root CAs from being trusted. This is particularly common on systems that are running MS-Vista.

Try to install SekChek's Root certificate manually, via the Certificate Import Wizard. (double-click on file SekRoot.cer, which is located in SekChek's installation directory)

If your system prevents third-party Root CAs from being trusted, Windows-XP may display one of the following messages:

- "An error occurred during the addition of a certificate to the Trusted Root Certification Authorities store."
- "The import failed because the store was read-only, the store was full, or the store did not open correctly."

With MS-Vista your system may not display any error message, but the certificate may be installed in your system's Intermediate CA store, instead of the Trusted Root CA store. This may occur even though you explicitly requested the certificate to be installed in the Trusted Root CA store.

The solution is to amend policy to ensure your system trusts SekChek's Root CA (only) *or* all third-party Root CAs.
Error 'Setup fatal error: Unable to generate installation log file' when installing the SekChek software

This error typically occurs if the account being used to install the SekChek Client software does not have Write permissions on Folder 'C:\Windows\'. The Setup routine uses this Folder to store its bootstrap / temporary installation files.

You can check this by viewing the security permissions on your system's C:\Windows\ directory (right-click on the Folder | Properties | Security Tab).

The solution is to install the SekChek software with an account that has sufficient permissions for the Folder.

SekChek's Help file (sekchek.chm) does not display properly

The majority of problems that prevent SekChek's Help file from displaying correctly are caused by security settings on your PC. The most common error messages are:

Error: The page cannot be displayed

Cause: Security settings are preventing executable files (e.g. EXE, CHM files etc) located in other domains from being executed on your PC. This occurs for example, when you try to open file SekChek.chm directly from SekChek's web site. This is normal / good practice for security.

Solution: Download the Help file (SekChek.chm) to a local drive on your PC and open the file from there.

Error: Navigation to the webpage was cancelled



Cause: Security settings are causing executable files downloaded from other computers to be 'blocked' in order to protect your PC. This occurs for example, when you download file SekChek.chm from SekChek's web site. This is normal / good practice for security.

Solution: You must manually unblock the Help file. To do this: right-click on file SekChek.chm; select Properties; select Unblock; click OK. The Help file should now open correctly.

Attributes:	🗖 Read-only 🔲 Hidden	Advanced
Security:	This file came from another computer and might be blocked to help protect this computer.	Unblock
	OK Cance	Apply

What are the minimum system requirements for the *SekChek* Software?

The <u>SekChek Client Software</u> requires Windows 2000 with Internet Explorer 5 (or later).

The <u>SekChek Scan Software</u> will run on *all* current versions of OS/400, Windows NT SP4 or later, Windows 20xx, UNIX operating systems and on Novell/NetWare systems, including:

- OS/400 V2R3 to V7R2
- UNIX-variants Sun/Solaris, HP-UX (including C2/TCB), DG-UX, OSF, SCO, AIX, UnixWare, Dynix, BSD, HI-UX, Nokia IPSO and Linux. *SekChek* for UNIX will run on any system that supports the Bourne shell
- Windows NT 4.0 Service Pack 4 or higher, Windows 200x, 20xx
- Novell/Netware 4 and later releases

If you would like to know more about *SekChek's* Software features, please <u>contact</u> us for more information.

What are the licensing restrictions on the software?

Quite simply, NONE! Although we retain the title and ownership of the *SekChek* software, you are free to use and to distribute the software in its *current form* to anyone you wish.

However, you are *not* allowed to attempt to modify, translate, reverse engineer, disassemble, or to create derivative works based on the software without the prior written consent of *SekChek*.

What is the Client software, Scan software & Processing Engine?

The Client software

The Client software contains usage instructions, encryption/decryption software and sample reports and the ability to generate copies of the Scan software. It typically resides on your PC.

SekChektor UNIX e View Ontions Tools Help		
AS/400 Netware UNIX	Windows	Utilities
Create Scan Software Create Scan software for execution on a UNIX system (any variant that supports the Bourne shell) Create		
2. Run the Scan		
Scan security on a UNIX system		
3. Encrypt Scan file		
Encrypt Scan files using Public Key Encryption Encrypt		
4. E-mail Scan file		
E-mail encrypted Scan files to inbox@sekchek.com		
5. Processing at SekChek	View Encrypted File Header	
Process your encrypted Scan files; compare security against industry averages; return your encrypted report package	Drag a SekChek file here to vie Drop a file anywhere on the fo	ew its EFH orm to process it
6. Decrypt report package		
Decrypt your encrypted SekChek report package Decrypt		
olic Key Encryption: ON (Encrypt to .SCK files)		

The Scan software

You use the Scan software to scan security data on a AS/400 (iSeries), NetWare, UNIX, Windows NT/200X system. It will only run on those systems.

SekChek for Windows	- 0 🔀
<u>File</u> <u>T</u> ools <u>H</u> elp	
SECURITY EVALUATOR Version 5.0.6 (01-Oct-2011)	
_ Waiting	
User Account: JoeSoap Computer Name: MyDC Windows Version: 6.0 Machine Role: PDC Member of Domain or Group: MyDomain DC for the Domain: MyDC	
Is this the system you want to analyse?	
To continue, click Next.	
Implications Change Directory < Back Next > Copyright & Trademarks Copyright @ 1996-2011 SekChek IPS. SekChek is a registered trademark of SekChek IPS. All other trademar property of their respective owners. This software is distributed free of charge. You are entitled to make any number of copies of the software a in its current form to anyone you wish.	Exit arks are the and to distribute it

The Processing Engines

The Processing Engines are used by the *SekChek* team to process your Scan file, to calculate <u>industry averages</u> and comparisons, and to generate and encrypt your *SekChek* reports.

What impact will SekChek have on my system?

From the very outset *SekChek* was designed to be non-intrusive, make ZERO changes to the host/target system, and leave no trace behind after the Scan process has completed. With 20 years experience and more than 80,000 successful Scans behind us, we are not aware of any incident where *SekChek* has caused problems on a host system – as long as it is executed in accordance with the standard operating instructions.

If there are concerns about the impact *SekChek* may have on system *performance*, our advice is to run the Scan software outside of peak processing time. This is especially applicable to UNIX systems with large file systems, to NetWare systems with large numbers of accounts, and to AS/400 systems with numerous programs that adopt authorities.

The SekChek for Netware and Windows software contain a convenient <u>Scheduler</u> facility, which allows you to run SekChek at some future point in time.

How long does SekChek take to run?

This is a difficult one to answer.

SekChek's execution time is dependent on many factors, such as CPU speed and system activity as well as the number of user accounts or files on the machine. However, here are some rough estimates, which should be accurate in 80% of cases.

SekChek for NetWare typically runs for 5-15 minutes on systems with up to 500 accounts. However on *very* busy, large systems (e.g. 10,000 accounts), you should allow 2-4 hours.

SekChek for Windows typically runs for 1-2 minutes on systems with up to 500 accounts. On large Active Directory domains (10,000+ accounts) it could run for 15 minutes or more. For Active Directory domains the execution time will also increase on domains with many containers/organization units and objects such as computer accounts.

Note that the option to 'query all Domain Controllers' for users' last logon information will significantly increase the execution time if the domain has a large number of Domain Controllers.

SekChek for UNIX typically runs for 5-10 minutes. However, if the host has a *very* large file system and you decide to scan details of world-writeable files or to scan files on NFS-mounted volumes, it could run for several hours. Note that steps with the potential to execute for a long time have all been made optional.

Can I schedule a SekChek Scan to run later?

Yes.

The *SekChek* for Netware and Windows Scan software contain a convenient Scheduler facility, which allows you to run *SekChek* at some future point in time. This is useful if you want to run *SekChek* outside prime business hours.

Click the <u>'Start Later' button</u> during the Scan process to invoke the Scheduler.

How do I drag / drop files to initiate processes?

Simply drop any *SekChek* file onto the main menu. *SekChek* will automatically start the relevant process, such as Encrypt, Email or Decrypt.

You can view an encrypted file's EFH or the embedded run-time options in the Scan software by dragging the file into the 'View Encrypted File Header' box on the main menu.

You can also initiate the File Splitter and SekCrypt utilities by dragging any file into the relevant utility box.

What security standards does SekChek measure against?

SekChek typically measures against *leading practices* for security because that's what most people want.

However, some clients prefer us to substitute their own (internal) security standards and to report against those. This helps them monitor how well their security policy is implemented and complied with. It also alerts management to deviations from policy in specific departments or on certain computers.

We have a database of real/actual industry averages for security. This is quite unique. We can currently compare (graph) security over different points in time, over several machines, and calculate security norms and averages by machine size, industry type and geographical location. This often produces some interesting results!

Contact us for further details.

Where do *SekChek's* Industry Averages come from?

Perhaps the most important point is that they are not merely based on a static, theoretical average for computer security.

30 million security measurements from 120+ countries...

SekChek's Industry Averages are dynamic, real-life averages that are automatically updated after each file we process using summary data obtained from each Scan file. Our statistics database contains more than 70,000 anonymous records from 120 different countries and in excess of 30 million individual security measurements.

Check out the Summary pages of your next *SekChek* report. The machine analysed was probably evaluated against *all* industry types and *all* countries. It will also have been evaluated against other similar-sized machines (based on the number of user accounts on the machine).

Then check your next *SekChek* report, or ask us to compare the same machine against a particular industry type. You should see some interesting differences in the graphical summary reports which will help you to understand just how dynamic these industry averages really are!

Why do *SekChek* reports keep changing?

We are continually researching better ways of analysing and reporting on security and improvements are added to the Processing Engines on a regular basis. The version of the Processing Engine that generated your report appears at the bottom of each page.

Many of the ideas and suggestions for improvement come from you, our customer. We welcome any suggestion or complaint and will do our best to incorporate your requirements into future releases of the software.

What formats can I have my *SekChek* report in?

SekChek reports can be generated in Word 2000 to Word 2010 formats.

The Word 97 format is compatible with most commonly available word processing software. However, if you would like your report in a different format, simply indicate your preference via the 'Options' screen in the *SekChek* Client software.

Because some *SekChek* reports can be very large, we also <u>provide you with the</u> <u>option</u> of having report Detail Sections greater than a specified size in MS-Access tables or Excel spreadsheets.

If you select one of these options you will receive a 'skeleton' (lean) main report in MS-Word format, with references to the large Detail Sections in Access or Excel format. You can even tell us where you would like the 'cut-off' point (e.g. 0 lines, 200 lines) to be. Only Detail Report Sections greater than this size will be sent to Access tables or Excel spreadsheets.

SekChek reports in these formats mean you have the ability to sort data according to your own particular requirements and to create your own personalised analyses via Query or Macro programs.

The choice is yours!

Can SekChek analyse Registry keys and NTFS permissions?

Yes.

SekChek can report on values for System Registry keys and analyse DACLs (Discretionary Access Control Lists) and SACLs (System Access Control Lists) for files and directories.

You do this by defining the list of the Registry keys, and the names of the files and directories you want to analyse in file **sekchek.inp**. See <u>SekChek for</u> <u>Windows Scan instructions</u> for details.

Must I forward my password each time I send a file to you?

No.

Your password is not used to encrypt Extract files. Your files are encrypted with *SekChek's* Public-Key using enhanced encryption techniques and your password is automatically included inside the encrypted package.

However, you will require your password to unlock the encrypted package containing your *SekChek* report. See <u>Public-Private Key Encryption</u> for more information.

How do I manage multiple Scan files?

If you have several similarly-named Scan files we recommend that you:

• Encrypt each Scan file separately (i.e. do not for example, bundle several Scan files together into a single ZIP file)

• Send your encrypted Scan files for processing in separate emails (the Encrypt & Email functions in the SekChek software will automatically handle this for you)

This practice will reduce the potential for misunderstandings and help prevent delays in the processing of your reports.

Encrypted Scan files and Report packages (e.g. SEKxxF.ZIP and SEKxxR.SDE)

Note that you can include your own descriptive text in the name of your Scan files and Report packages. *SekChek* will recognise these extended filenames as long as you retain *SekChek*'s 6 character prefix. E.g.:

- SEKxxF MyHost 20070316.ZIP
- SEKxxR YourDescriptiveText.SDE

(where xx is SekChek's system identifier. E.g. AS, NE, UN or WI)

Can I run *SekChek* if the target machine has no diskette drive?

Yes.

With *SekChek* for Windows, you can copy the Scan software to a directory on the Server, or to a directory on a workstation attached to the Server. You can even run it from a diskette drive on a workstation attached to the Server.

However, you must then *logon (locally) to the Server*, and execute the software from the remote drive or directory. You will get incorrect results if you logon to the workstation and *execute* the software from there.

With *SekChek* for UNIX, the best way is to logon to a workstation and use *ftp* to transfer the Scan software to a directory on the target (UNIX) machine. To ensure correct results, you must remember to transfer the software in *binary* (not ASCII) mode.

With *SekChek* for NetWare the question does not apply because the Scan software is not run from the Server. You must run it from a Client 32 workstation (running Windows 200X) attached to the network.

What's the difference if I run SekChek for Windows on a Domain Controller, Server or Workstation?

SekChek automatically recognises the type of machine it is running on and changes the scope of the analyses accordingly. For example, if *SekChek* is run on a Domain Controller, it will analyse domain-wide security settings, RAS access to the domain, and all user accounts defined in the domain controlled by that Domain Controller.

If *SekChek* is run on a non-DC Server or a Workstation, it will analyse security settings and user accounts applicable to that specific machine only.

A very comprehensive view of security can be obtained by running *SekChek* on a Domain Controller for a domain, on the Servers or Workstations that contain the most sensitive applications and data, and on any trusted domains.

For more information please read the Help section <u>Planning Your SekChek for</u> <u>Windows Analysis</u>.

How are *SekChek* files from Windows & NetWare systems encrypted?

The Scan software for *SekChek* for Windows and NetWare automatically encrypts your Scan files on the target machine using symmetric encryption techniques. However, for additional security we recommend that you use <u>SekChek's Public/Private Key Encryption</u> features.

These features employ industry-standard encryption techniques and algorithms, such as RSA and DES and are available via the Client software on your PC. You can enable them by turning on (checking) the 'Public Key Encryption' option on the Options page of the Client Software. Please refer to the Encryption Instructions for more details.

Can we exchange encrypted email (S/MIME, SSL or TLS) with SekChek?

Yes, our Mail servers are configured to send and receive email using TLS (Transport Layer Security / SSL).

If the TLS protocol is enabled on your Mail server all email traffic between SekChek's domain and your organisation's domain will be automatically encrypted.

SekChek also supports S/MIME, which ensures full end-to-end encryption of email. You can download SekChek's certificate from our <u>web-site</u>.

Let us know if you need more information regarding options for encrypting email.

What about security over SekChek files after they are processed?

We obviously appreciate the sensitivity of the data contained in *SekChek* files and reports, so we have implemented very strong controls to ensure they remain confidential and are promptly removed from our system after processing. For example:

- By default, all Client data (Scan data and Report files) is automatically deleted from our system after 5 days. Let us know if you want to define a shorter retention period.
- During this period, client data is stored in encrypted format and protected against unauthorised access.
- We do not publish or divulge the address of our Processing Centre.
- Access to our premises and Servers is controlled by several layers of physical security controls.
- Stringent background checks are performed on all potential employees.
- All employees sign a strict confidentiality agreement / NDA on an annual basis.
- Our disciplinary code defines a zero-tolerance approach towards acts of dishonesty and poor ethics.
- All printed material is shredded and burnt. *SekChek* reports are not printed.
- We abide by the same professional rules of conduct that exist between an auditor & his client.
- Security controls over *SekChek* files and reports are stronger than similar controls over most other confidential client data.
- Our security procedures are independently audited on a regular basis.

What if a client's security policy prevents *SekChek* files from being sent outside an organisation?

The <u>Mobile-SekChek</u> service has been created to allow a senior security consultant to travel to the client's premises and perform the SekChek analysis onsite. This means that SekChek reports can be produced without sensitive data ever leaving the client's premises.

You can also use the *SekChek Local* range of products, which allow you to process Scan data locally, without having to send data off-site for processing.

SekChek Local allows you to analyse multiple Hosts in a single scan and runs on a regular PC attached to your network. Visit our <u>web site</u> or <u>write to us</u> for details.

Will *SekChek* work on systems running third party security software?

In *most* cases the answer is yes.

This is because most third party security systems are designed and built on the host system's native security files and methods - they just improve on the basic principles.

However, some products, such as *Guardian* (on UNIX systems) use their own special files and formats. If this type of product is used on the target machine, the *SekChek* Scan software will still run, but some of the reports will be incomplete because they will not take into account the extra data in these special files.

If in doubt, either ask us for our opinion, or just go ahead and run *SekChek*. If you are not satisfied with the results simply let us know and we will not charge you for the analysis.

What payment options are available?

Direct (Bank-to-Bank) transfer

This is the preferred option. In general, it is the quickest and safest payment method.

Cheque payment

If you prefer to make payment by cheque we recommend that you send your cheque via a courier company, rather than the regular postal system.

We have special arrangements in place with UPS, Fedex and DHL, which help to speed up the process.

Credit Card payments

We offer a secure Credit Card payment system managed by Kagi.

If you are interested in making your payment via Credit Card please let us know.

Write to us for more information on any of these payment methods.

Tell me about your subscription service!

The most convenient & cost effective way to use *SekChek* is through a subscription. The pricing structure is very simple - the more *SekChek* units you subscribe to, the less the cost per unit / report. Contact us for details of <u>payment</u> <u>options</u> and the latest pricing.

Prices are consistent across the entire *SekChek* range (AS/400, NetWare, Windows & UNIX), so you only need purchase one subscription. You are free to choose and mix different *SekChek* services in the same subscription.

Once your subscription is confirmed you just send us your security files for processing any time you are ready. We will send you a statement indicating your usage of *SekChek* on a monthly basis. We will also issue a reminder just before your subscription is consumed. Subscriptions have no time limits attached to them.

Can I offer *SekChek* to a client of mine?

The answer is a definite *YES*. The majority of our clients are gained by referrals from existing clients. Your client can arrange a subscription through yourself or by contacting us directly.

Organisations choose to use *SekChek* for many reasons. These include *SekChek's* unique ability to bench-mark their security measures against real-world security standards by industry type and location, savings in time & the cost of performing detailed security reviews, the consistency of the analyses, and the easy-to-read, graphical report summaries that are presented in a non-technical format.

Many organisations run *SekChek* on a regular basis, so they can monitor any changes in the strength of their security measures over different points in time. They also want to keep tabs on how they are doing compared with the competition!

What are your plans for SekChek?

Our guiding principles are ease-of-use and interpretation; non-intrusiveness on the host machine; value for money; and speed of delivery.

Some of the more specific areas we are focusing on include improved graphical summaries, trend analyses (<u>spanning time</u>, machines, departments etc.), and <u>'industry average' bench-marks</u> by industry type and geographical location.

The direction the *SekChek* service takes is largely determined by your requirements and needs. Tell us what you want!

How do I make the best use of *SekChek*?

You have mentioned lots of great ideas to us, many of which are listed in this FAQ. Some others worth a mention are:

DO use *SekChek* as early as possible in an assignment. The *SekChek* report will help you focus and leverage your time better. Many consultants send *SekChek* to their client well before they start an assignment and request the client to forward the files directly to us. This saves you and your client both time and money.

DO use the (graphical) summary reports for highlighting trends in the strength of security over time and across different computers and departments. They help answer questions such as "Is security getting better or worse?", "Which computer has the strongest/weakest security" and "Where does security not comply with policy?".

DO call us if you have difficulty with any part of the *SekChek* process. We try to make the process as hassle-free as possible, but there may be the inevitable hiccup or problem. If you don't tell us about your difficulties, we will not be able to fix them.

DO call us with your questions. The preferred medium is e-mail & we aim to answer most questions within 2 hours of receipt.

DO tell us what improvements you would like to see. We will do our best to include your requirements in a future release of the software.

DON'T expect *SekChek* to provide all the answers. Certain types of question require some understanding and knowledge of the client's business. An obvious example is: "Should John Smith in the Finance department have access to XXX?". However, we would be very disappointed if you find that *SekChek* does not at least 'break the back' of a security review.

How do I remove *SekChek's* digital certificate?

If you enabled *SekChek's* Public Key Encryption features, the software will have automatically installed SekChek's digital certificate in your system's certificate store.

To remove the certificate, please do the following:

▲ Warning: The X.509 digital certificate is an essential component of *SekChek's* <u>Public Key Encryption</u> features. If you remove the certificate from your system, you will not be able to encrypt Scan files with *SekChek's* Public Key.

1. Select the Content Tab of Internet Options in Internet Explorer



2. Click Certificates on the Content Tab

stued To	Issued By	Expratio	Prioridy N
SeiCet	SelChelSubOrdhate.	17560-2	dane>
ſ			
port _ Diport.	Beaches		onevtě.

3. Remove SekChek's Certificate

Select the **Other People** tab

Select the certificate issued to SekChek

Click Remove

Click **Yes** when prompted to delete the certificate

6. Close Internet Explorer

Click **Close** to exit the Internet Explorer Certificate window.

SekChek's digital certificate has now been successfully removed from the system.

✓ Note:

If you decide to use the Public Key Encryption features at some later stage, simply enable the **Use Public Key Encryption** option, which is on the **Options** screen of the *SekChek* Software. This will ensure that *SekChek's* certificate is installed in the appropriate certificate store on your system.

If you would like to know more about *SekChek's* X.509 digital certificates, please <u>contact</u> *SekChek* for more information.

Limitation of Liability

Under no circumstances and under no legal theory, tort, contract, or otherwise, shall *SekChek*, any of its members, nor anyone else who has been involved in the creation, production or delivery of this software be liable to you or any other person for any indirect, special, incidental, or consequential damages of any kind including, without limitation, damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other damages or losses. In no event will *SekChek* be liable for any damages even if *SekChek* has been advised of the possibility of such damages, or for any claim by any other party.

General

Expand all Leading Practice

This represents the generally accepted, international standard for security; the standard to strive for.

Client Software

The Client software contains usage instructions, encryption/decryption software, sample reports and the ability to create additional copies of the Scan software. It typically resides on your PC.

Encrypted File Header (EFH)

All files encrypted by *SekChek* (as well as the *SekChek* for Windows & Netware Scan software) contain an EFH. The EFH contains general information about the file such as:

- The name and size of the source file
- A date/ time stamp indicating when the file was encrypted
- A unique identifying FileID
- *SekChek's* own RefNbr (if the file is an encrypted report package).

• The default processing & run-time options (contact details, report format, evaluation options etc) that were selected when you created the *SekChek* for Windows / Netware Scan software.

• Run-time options that were selected during the Scan process. E.g. 'Query all DCs for users' last logon details' on Windows systems and 'Analyse files with world writeable permissions' on UNIX.

This information is useful for tracking and identification purposes.

You can display a file's EFH by dragging the file into the 'View Encrypted File Header' box on the main menu or:

- 1. Selecting the file via the Decrypt function or the SekCrypt utility; and
- 2. Checking the 'Display File Header' checkbox

Encryption Password

The password that was entered during the encryption process. This password is used to encrypt your *SekChek* report.

Scan Software

The Scan software is used to scan security on an AS/400, NetWare, UNIX or Windows NT/2000/2003/2008 target machine. It will only run on those systems.

Industry Average

SekChek's industry averages for security are real-life averages that are recalculated after each security file we process. This makes them very dynamic, so they will change depending on selection criteria such as industry type and country.

Options and Settings

See **Option Values**

Processing Engine

The Processing Engine is used by the *SekChek* team to process Scan data, to calculate industry averages and comparisons, and to generate and encrypt *SekChek* reports.
Public Key Encryption

Public Key Encryption is an encryption technique that uses a pair of keys to encrypt and decrypt data. For more information, refer to <u>SekChek's Public Key</u> <u>Encryption</u>.

Reference Number

The Reference Number is a unique number assigned to each analysis performed by *SekChek*. The Reference Number can be found on the Options page in every *SekChek* report as well as in the subject line of the emails sent back to you with your File Receipt and *SekChek* Report.

Self-Extracting Software

This is a self-extracting executable, which is used to set-up and install the *SekChek* Client software on a Windows PC. It is always called SEKxxx.EXE, where 'xxx' represents the version number. E.g. SEK473.EXE.

SekChek® is a registered trademark of SekChek IPS. All other trademarks are the property of their respective owners.

AS/400

Expand all Adopted Authority

AS/400's Adopted authority feature allows users to adopt the authority of a program's owner while the program is running. It allows users to be given *temporary* (indirect) authority to objects, while under the control of a program with restricted functionality, rather than having *permanent* and direct access to the objects concerned.

ANZDFTPWD

The program called that returns a listing of all user profiles that have their password equal to their profile name.

Attention-Key Programs

The program called when the user presses the Attention key. The program may allow the user, for example, to gain access to the command line.

Data Authorities

Define the operations that can be performed on the contents of an object. Also see 'Object Authorities'.

Group Profile

Group profiles are used to give multiple users the same set of access authorities. Authorities defined to a Group profile are overridden by those defined in the User profile.

IBM-Supplied Profiles

Some types of profile, such as Group profiles and some of the IBM-supplied (Q.) profiles, are not normally used to sign-on to a system. They are typically used for grouping together those users with similar access requirements, or used internally by OS/400 itself.

Initial Programs and Menus

An Initial Program is often used to set up the application environment or ensure the user can only run one program and never sees a menu. The Initial Menu is the first menu the user sees after signing on to the system. It is displayed after the user's Initial Program has executed.

Limited Capability

Limited Capability can be set to control the users ability to change their Initial Program, initial Menu and current library.

<u>OBJAUT</u>

The *SekChek* output file for Object Authorities. The file is called 'objaut.txt'. See also 'Object Authorities'.

Object Authorities

Define the operations that can be performed on an object as a whole. Also see 'Data Authorities'.

PGMADP

The filename given by *SekChek* for 'Adopted Authorities' data. The file is called 'pgmadp.txt'. See also 'Adopted Authority'.

PROFBAS

The filename given by *SekChek* for data on profiles and important related information. The file is called 'profbas.txt'.

SEKASF.SCK

The filename given by *SekChek* to the set of compressed and encrypted files extracted from AS/400 systems. SCK files are encrypted with *SekChek's* Public Key using industry-standard algorithms, such as RSA and 3-DES. They can only be decrypted at *SekChek's* premises with the corresponding non-exportable Private Key.

SCK files are created when the 'Public Key Encryption' option is enabled in the *SekChek* Client software on your PC. This is the recommended option.

SEKASF.ZIP

The filename given by *SekChek* to the set of compressed and encrypted files extracted from AS/400 systems.

ZIP files are created when the 'Public Key Encryption' option is disabled (unchecked) in the *SekChek* Client software on your PC. For improved security, we recommend that you enable this option. Refer to the definition of SEKASF.SCK files for more information.

SEKASR.SDE

The filename given by *SekChek* to the set of compressed and encrypted files containing your *SekChek* reports. SDE files are symmetrically encrypted with industry-standard algorithms, such as DES.

<u>SEKLOG</u>

The filename given by *SekChek* for *SekChek's* logfile. The file is called 'seklog.txt'.

Simultaneous Device Sessions

The capability of signing-on to multiple workstations at the same time.

Special Authorities

The authorities (rights) assigned to profiles (group or user) defined to the system. I.e. they include Special Authorities granted directly to the profile as well as authorities that are inherited indirectly through Group membership. An example of a Special Authority is the right to 'Access all system resources'.

SRVTBLE

The filename given by *SekChek* for data listing active 'System Services'. The file is called 'srvtble.txt'.

System Values

The system-wide security defaults (System Values) defined for the system. System Values can be seen as the default policy settings for the system. They can be overridden at profile level. An example is the default 'Minimum password length' which is set with the system parameter 'QPWDMINLEN'.

SYSVALS

The filename given by *SekChek* for the 'System Values' data. The file is called 'sysvals.txt'. See also 'System Values'.

User Classes

When created, user profiles belong to a 'User Class'. Different 'User Classes' will grant certain default rights to the user. For example, a 'User Class' of SECADM will grant powerful rights (Special Authorities) by default. See also 'Special Authorities'.

<u>User Profile</u>

A user profile is the user account with all its associated privileges and settings for a user. See also 'Group Profile'.

SekChek® is a registered trademark of SekChek IPS. All other trademarks are the property of their respective owners.

NetWare

Expand all Admin

Usually the account that has full Administration rights. When a NetWare system is set up the Admin account is automatically created.

<u>Alias</u>

An Alias object points to another object in the Directory tree. It makes it appear that the object that it references actually exists in the part of the Directory tree where the Alias is created. The purpose of an Alias is to allow users to work with the object the Alias points to without having to change to the object's context.

Container

An object that contains other objects in the Directory tree. An example is an Organization Unit which contains user objects.

<u>Context</u>

The path (location) of an object in a Directory tree.

Grace Logins

Grace Logins allow a user with an expired password to continue signing-on until his/her Grace Logins are consumed. The Grace Login count is decreased by 1 each time a user with an expired password logs on without changing his/her password.

Groups

Groups and Roles are objects in the directory tree. They provide a convenient way to give several users the same set of Rights and privileges. Access rights assigned to Group and Role objects are added to rights that are directly assigned to member Users via their user accounts.

Intruder Detection

Intruder Detection features play an important role in controlling the risk of unauthorised access to a system via repeated password guessing attempts. Depending on the settings, Intruder Detection can, for example, lock out accounts which have exceeded a set number of invalid logon attempts.

Objects

Entities defined in the Directory tree. Groups, Organization Units, Computers, Volumes, Users etc.. are all objects. Objects which contain other objects are known as Containers.

<u>Roles</u>

See Groups.

Root

The highest level in the tree. The root of the Directory tree.

Security Equivalence

A User object that is security equivalent to other objects automatically inherits the Rights of those objects. These inherited Rights are added to those Rights that are directly assigned to the User object.

SEKNEF.SCK

The filename given by *SekChek* to the set of compressed and encrypted Scan files from a NetWare system that have been encrypted using *SekChek's* 'Public Key Encryption'. SCK files are encrypted with *SekChek's* Public Key using industry-standard algorithms, such as RSA and 3-DES. They can only be decrypted at *SekChek's* premises with the corresponding non-exportable Private Key.

SCK files are created when the 'Public Key Encryption' option is enabled in the *SekChek* Client software on your PC. This is the recommended option.

SEKNEF.ZIP

The filename given by *SekChek* to the set of compressed and encrypted Scan files from a NetWare system.

For improved security, we recommend that you encrypt this file using *SekChek's* 'Public Key Encryption'. Refer to the definition of SEKNEF.SCK files for more information.

SEKNER.SDE

The filename given by *SekChek* to the set of compressed and encrypted files containing your *SekChek* reports. SDE files are symmetrically encrypted with industry-standard algorithms, such as DES.

Simultaneous Device Sessions

The capability of signing-on to multiple workstations at the same time.

Supervisory Rights

The rights granted to an object over another object. Most objects can be granted supervisory rights over other objects.

SekChek® is a registered trademark of SekChek IPS. All other trademarks are the property of their respective owners.

UNIX

Expand all C2 Security

A term generally applied to UNIX systems with 'Enhanced Security' where security features allow the system to meet the standards of a C2 security rating.

The National Computer Security Center (NCSC) established a process by which software vendors can submit their security-related products for evaluation.

NCSC Security ratings range from 'A' to 'D,' where 'A' represents the highest security level. The 'C' rating is generally applied to business software. Each rating is further divided into classes. For example, in the 'C' division, software may be rated either 'C2' or 'C1,' with 'C2' representing the higher security.

<u>GID</u>

Internally, UNIX identifies groups by their numeric GID (Group Identifier), rather than their group names.

Groups

Group profiles provide multiple users with the same set of access permissions and privileges. Access permissions assigned to group profiles are added to permissions that are directly assigned to Users that are members of a Group.

Passwd File

UNIX uses the 'passwd' file (normally found in the path /etc/passwd) to keep track of every user on the system. The file contains the username, real name, identification information and basic account information for each user. On UNIX systems with basic security the file also contains users' encrypted passwords. See also 'Shadow Passwd Files'.

Remote Login

The ability to access the system remotely via, for example, the telnet terminal network service. The ability to login remotely can be granted or denied to users.

<u>Root</u>

Every UNIX system comes with a special account with a UID of 0. This account is known as the superuser and has a username of *root*. The *root* account is used by the operating system itself to accomplish many of it's functions. For this reason, the superuser has nearly complete control over the operating system. Most security checks are turned off for any program that is run by the *root* user.

<u>sekunf.z</u>

The filename given by *SekChek* to the set of compressed Scan files extracted from UNIX platforms before encryption by *SekChek*. See also SEKUNF.ZIP.

SEKUNF.SCK

The filename given by *SekChek* to the set of compressed and encrypted Scan files extracted from UNIX platforms. SCK files are encrypted with *SekChek's* Public Key using industry-standard algorithms, such as RSA and 3-DES. They can only be decrypted at *SekChek's* premises with the corresponding non-exportable Private Key.

SCK files are created when the 'Public Key Encryption' option is enabled in the *SekChek* Client software on your PC. This is the recommended option.

SEKUNF.ZIP

The filename given by *SekChek* to the set of compressed and encrypted files extracted from UNIX platforms.

ZIP files are created when the 'Public Key Encryption' option is disabled

(unchecked) in the *SekChek* Client software on your PC. For improved security, we recommend that you enable this option. Refer to the definition of SEKUNF.SCK files for more information.

SEKUNR.SDE

The filename given by *SekChek* to the set of compressed and encrypted files containing your *SekChek* reports. SDE files are symmetrically encrypted with industry-standard algorithms, such as DES.

Sensitive Directories

In *SekChek*, sensitive directories include those containing files that determine the operating environment and security rules for a service.

Sensitive Files

In *SekChek*, sensitive files include security and system configuration files, files in the System Search Path and sensitive user files, such as 'rhosts' and 'profile'. Examples are 'Passwd Files', 'Shadow Passwd Files' and programs such as the program that changes user passwords. Many of these files contain statements that are 'executed' by the system when certain services are started and initialised.

<u>SGID</u>

A program that switches its GID (Group Identifier) when it executes.

It is sometimes necessary for a user to accomplish tasks that require privileges and permissions that his own userid does not have. One of the ways such programs achieve this is by assuming the privileges of a powerful GID (Group Identifier) when they execute. See 'SUID' also.

Shadow Passwd Files

Systems with *shadowing* features store users' encrypted passwords in a 'shadow'

passwd file, rather than the /etc/passwd file, which is typically world-readable. UNIX systems with C2 level security features also use *shadow* passwd files. See 'Passwd File' also.

<u>SUID</u>

Programs that SUID (Switch Userid) assume the privileges of another UID (User Identifier), such as *root*, rather than that of the user invoking the program.

An example is the program that changes a user's login password. While the user may not be able to edit the system's 'passwd file' directly, the *passwd* program can. This allows a user to perform privileged functions allowed by a special-purpose program, without assigning these privileges to the user on a permanent basis. Also see 'SGID'.

Trivial Passwords

Passwords that can be easily guessed. Examples are *AA*, a password equal to the username, and simple words such as *Monday*, *or January*.

Trusted Hosts

If one host (system) trusts another host, any user who has the same username on both hosts can log in from the trusted host to the other computer without entering a password. See also 'Trusted Users'.

Trusted Users

If a user on another computer is designated as a trusted user for an account on the current computer, the trusted user can login to the account on the current computer without entering a password.

<u>UID</u>

Internally, UNIX identifies users by their numeric UID (User Identifier), rather

than their user names. This means that the system 'sees' usernames with the same uid as the same user, so they are granted similar access privileges.

World-Writable Files and Directories

Files and directories that can be written to by any user on the system.

SekChek® is a registered trademark of SekChek IPS. All other trademarks are the property of their respective owners.

Windows Systems

Expand all Accounts Policy

The policy settings that set defaults for accounts in Windows Workstations, Servers and Domain controllers. The default settings address password controls and intruder lockout controls.

Active Directory (Windows 200X)

The Active Directory allows a single point of administration for all published resources, which can include files, peripheral devices, host connections, databases, Web access, users, other arbitrary objects, services etc.

It uses the Internet Domain Name Service (DNS) as its locator service, organizes objects in domains into a hierarchy of organizational units (OUs), and allows multiple domains to be connected into a tree structure.

Administration is further simplified because there is no notion of a primary domain controller (PDC) or backup domain controller (BDC) as in Windows NT. The Active Directory uses domain controllers (DCs) only, and all DCs are peers. An administrator can make changes to any DC, and the updates will be replicated on all other DCs.

Audit Policy

Selected activities of users and the system can be tracked by auditing security and other events and then placing entries in a computer's logs. The Audit policy settings determine the types of events that will be logged for the computer.

Backup Domain Controller (Windows NT)

A Backup Domain Controller (BDC) is a computer running Windows NT Server that receives a copy of the domain's security database containing account and

security policy information for the domain. The copy is synchronised periodically and automatically with the master copy on the primary domain controller (PDC).

BDCs also authenticate user logons and can be promoted to function as PDCs as needed. Multiple BDCs can exist in a domain. BDCs provide resilience and add to the effectiveness of the logon process, especially in networks where servers and users are geographically dispersed.

<u>BDC</u>

See 'Backup Domain Controller'.

<u>Domain</u>

A domain is a collection of computers defined by the administrator of a Windows Server network that share a common account database and security policy. A domain provides access to the centralised user accounts and group accounts maintained by the domain administrator. Each domain has a unique name.

Domain Controller

For Windows NT, see 'Primary Domain Controller' and 'Backup Domain Controller'.

A Domain Controller (DC), in a Windows 200X domain, is a computer running Windows 200X Server and Active Directory that authenticates domain logons and maintains the security database for a domain.

The DC tracks changes made to accounts, groups, policy and trust relationships in a domain. A Windows 200X domain can have more than one DC. For most management functions all DCs in a Windows 200X domain are equal and information is replicated between DCs.

Domain Trust

A trust relationship is a link between two Windows domains. Trusted Domains are domains that the current domain trusts to use its resources. Trust relationships can only be established between Windows domains.

Trusting domains allow their resources to be used by accounts in trusted domains.

Trusted domain users and selected types of groups can hold rights, resource permissions, and group memberships on the trusting domain.

Trust relationships allow users to access resources on the trusting domain using a single user account and a single password. The trusting domain will rely on the trusted domain to verify the userid and password of users logging on the trusted domain.

Drivers

See 'Services'.

Global Group (Windows NT)

For Windows NT Servers that are Primary or Backup Domain Controllers, a group that can be used in its own domain, member servers, workstations of the domain and trusting domains.

A global group can be granted rights and permissions in the above areas and can be a member of local groups, thus acquiring their rights. However, it can only contain individual user accounts from its own domain. Groups (local or global) cannot be members of global groups. User accounts must belong to at least one global group (their primary group).

Global groups provide a way to group together users with similar access requirements inside the domain. They are available for use both in and out of the domain.

Global groups cannot be created or maintained on Windows NT Workstations or Windows NT Servers that are not Primary or Backup Domain Controllers. However, for Windows NT Workstation or NT Server computers that participate in a domain, domain global groups can be granted rights and permissions at those workstations or servers, and can be members of local groups at those workstations or servers.

Global Group (Windows 200X)

For Windows 200X Servers that are Domain Controllers, a group that can be used in its own domain, member servers, workstations of the domain and trusting domains.

Groups with global scope can have as their members groups and accounts only from the domain in which the group is defined and can be granted permissions in any domain in a domain tree or forest.

In native-mode Windows 200X domains, Global Groups can have, as their members, accounts from the same domain and global groups from the same domain.

In mixed-mode Windows 200X domains, Global Groups can have, as their members, accounts from the same domain but cannot have groups as members.

Global groups cannot be created or maintained on Windows Workstations or Servers, that are not Domain Controllers. However, for Windows Workstations or Server computers that participate in a domain, domain global groups can be granted rights and permissions at those workstations or servers, and can be members of local groups at those workstations or servers.

Local Group (Windows 200X)

Groups with domain local scope can have as their members groups and accounts from Windows 200X or Windows NT domains and can be used to grant permissions only within a domain.

In native-mode Windows 200X domains, Local Groups can have accounts, global groups, and universal groups from any domain, as well as local groups from the same domain, as members.

In mixed-mode Windows 200X domains, Local Groups can have accounts and

global groups from any domain as members but cannot have local groups as members.

Groups with domain local scope are typically used to define and manage access to resources within a single domain.

For Windows NT/2000/XP Workstations and Windows NT/200X Servers that are not Domain Controllers, a local group can be granted permissions and rights for the workstation or server only. However, a local group can contain its own user accounts and, if the workstation or server belongs to a domain, user accounts and global groups (not local groups) both from the domain and trusted domains.

Member Server

A computer that runs Windows NT or Windows 200X Server but is not a Windows 200X domain controller or a primary domain controller (PDC) or backup domain controller (BDC) of a Windows NT domain. Member servers do not receive copies of the security database. See also PDC, BDC and Domain Controller.

Mixed Mode Domain (Windows 200X)

The default mode setting for domains on Windows 200X domain controllers. Mixed mode allows Windows 200X domain controllers and Windows NT backup domain controllers to co-exist in a domain.

Mixed mode does not support the universal and nested group enhancements of Windows 200X. You can change the domain mode setting to Windows 200X native mode after all Windows NT domain controllers are either removed from the domain or upgraded to Windows 200X. See also native mode domain.

Native Mode Domain (Windows 200X)

The condition in which all domain controllers within a domain are Windows 200X domain controllers and an administrator has enabled native mode operation (through Active Directory Users and Computers). See also mixed

mode domain.

<u>PDC</u>

See 'Primary Domain Controller'.

Primary Domain Controller (Windows NT)

The Primary Domain Controller (PDC), in a Windows NT Server domain, is the computer running Windows NT Server that authenticates domain logons and maintains the security database for a domain. The PDC tracks changes made to accounts, groups, policy and trust relationships in a domain. It is the only computer to receive these changes directly. A domain has only one PDC.

<u>RAS</u>

RAS (Remote Access Service) allows users to access the system or domain remotely via modems, ISDN etc.

Registry

The Windows NT registry is a database repository for information about a computer's configuration. It is organized in a hierarchical structure, and is comprised of subtrees and their keys, hives, and value entries. The Registry is a central repository which stores configuration information on things such as hardware, software and user accounts.

SEK2KF.SCK

The filename given by *SekChek* to the set of compressed and encrypted Scan files extracted from an Active Directory domain that have been encrypted using *SekChek's* 'Public Key Encryption'. SCK files are encrypted with *SekChek's* Public Key using industry-standard algorithms, such as RSA and 3-DES. They can only be decrypted at *SekChek's* premises with the corresponding non-exportable Private Key.

SCK files are created when the 'Public Key Encryption' option is enabled in the *SekChek* Client software on your PC. This is the recommended option.

SEK2KF.ZIP

The filename given by *SekChek* to the set of compressed and encrypted Scan files extracted from an Active Directory domain.

For improved security, we recommend that you encrypt this file using *SekChek's* 'Public Key Encryption'. Refer to the definition of SEK2KF.SCK files for more information.

SEKWIR.SDE

The filename given by *SekChek* to the set of compressed and encrypted files containing your *SekChek* reports. SDE files are symmetrically encrypted with industry-standard algorithms, such as DES.

SEKNTF.SCK

The filename given by *SekChek* to the set of compressed and encrypted Scan files extracted from a Windows server that have been encrypted using *SekChek's* 'Public Key Encryption'. SCK files are encrypted with *SekChek's* Public Key using industry-standard algorithms, such as RSA and 3-DES. They can only be decrypted at *SekChek's* premises with the corresponding non-exportable Private Key.

SCK files are created when the 'Public Key Encryption' option is enabled in the *SekChek* Client software on your PC. This is the recommended option.

SEKNTF.ZIP

The filename given by *SekChek* to the set of compressed and encrypted Scan files extracted from a Windows server.

For improved security, we recommend that you encrypt this file using SekChek's

'Public Key Encryption'. Refer to the definition of SEKNTF.SCK files for more information.

<u>Server</u>

In general, refers to a computer that provides shared resources to network users. See also 'Member Server'.

Services

A service is an executable object that is installed in a registry database maintained by the Service Control Manager. The executable file associated with a service can be started at boot time by a boot program or by the system, or the Service Control Manager can start it on demand. The two types of service are Win32 services and driver services.

A Win32 service is a service that conforms to the interface rules of the Service Control Manager. This enables the Service Control Manager to start the service at system start-up or on demand and enables communication between the service and service control programs. A Win32 service can execute in its own process, or it can share a process with other Win32 services.

A driver service is a service that follows the device driver protocols for Windows rather than using the Service Control Manager interface.

Shares

A share is a folder or printer resource on the local system that is accessible from a remote machine on the network.

Once a resource is shared, you can restrict its availability over the network to certain users. These restrictions, called *share permissions*, can vary from user to user.

Trusted Domain

See 'Domain Trust'.

Trusting Domain

See 'Domain Trust'.

Universal Group (Windows 200X)

Groups with universal scope can have as members groups and accounts from any Windows 2000/2003/2008 domain in the domain tree or forest and can be granted permissions in any domain in the domain tree or forest.

In native-mode Windows 2000/2003/2008 domains, Universal Groups can have, as their members, accounts from any domain, global groups from any domain and universal groups from any domain.

In mixed-mode Windows 2000/2003/2008 domains, groups with universal scope cannot be created.

Groups with universal scope can be used to consolidate groups that span domains. For example, global groups from different domains can be nested in universal groups. Using this strategy, any membership changes in the groups having global scope do not affect the group with universal scope.

User Rights

Define a user's access to a computer or domain and the actions that a user can perform on the computer or domain. User rights permit actions such as logging onto a computer or network, adding or deleting users in a workstation or domain.

<u>Workgroup</u>

A workgroup is a collection of computers that are grouped for browsing purposes and sharing of resources. Each workgroup is identified by a unique name. A workgroup is not a domain and does not have centralised user accounts or a common security policy. Each computer in the workgroup maintains its own set of accounts, groups and security policy.

Workstation

Any networked PC using server resources. See also 'Member Server', 'Domain Controller', 'Primary Domain Controller' and 'Backup Domain Controller'.

SekChek® is a registered trademark of SekChek IPS. All other trademarks are the property of their respective owners.

What is the largest system analysed by SekChek?

The largest domain analysed by SekChek contained more than 430,000 user *accounts* and the security reports and benchmark summary were produced within a few hours of completion of the Scan.

You may be interested to know that to date, SekChek has analysed 75 *million user accounts* and 25 *million security groups* on systems belonging to many of the world's largest and best known organisations.

Some other interesting statistics are:

- 45 million network attached Servers and workstations
- 7 million Windows services
- 180,000 locally attached disk drives
- 280 million DACLs
- 1.5 million hot-fixes
- 1.1 billion file permissions

There is no limit to the size of system that SekChek can analyse.