Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Overview of the Windows 2000 Security Tools

Windows NT has some excellent security tools and features built into the operating system. In addition the operating system provides tools for security policy and account management and the Windows NT security model is flexible and can support a wide range of configurations. However, these tools are not centralized and the administrator needed to open three or four applications to configure various aspects of security. Using these tools can sometimes be difficult and complex at best. Additionally, with the distributed ...

Copyright SANS Institute
Author Retains Full Rights

AD

Beating the IPS?

STONESOFT
Can't be Beat

Learn More

Windows 2000 Built–in Security Tools
Jeff Christman

INTRODUCTION:
Windows NT has some excellent security tools and features built into the operating system. In addition the operating system provides tools for security policy and account management and the Windows NT security model is flexible and can support a wide range of configurations.

However, these tools are not centralized and the administrator needed to open three or four applications to configure various aspects of security. Using these tools can sometimes be difficult and complex at best. Additionally, with the distributed security model in windows 2000, the complexity has only increased. While NT provided adequate, if inconvenient, configuration tools, it lacked tools for security analysis.

Windows 2000 builds on the NT security model and expands it to provide a comprehensive, flexible and extensible set of tools. Also, taking advantage of MMC technology, it provides a central administration point for the tool set by making the tools available as MMC snap–ins. Windows 2000 also add many tools that were lacking in the NT operating system.

This paper will describe the location and use of the tools that are built into Windows 2000 operating system. With these tools, the administrators have a greater degree of control and can provide a secure internet- aware enterprise without purchasing third party tools.

<u>Using the built in tools</u>

Tool: The Security Configuration Tool Set
Location: Installed as part of the operating system

The Security Configuration Tool Set is a set of MMC snap-ins that offers a comprehensive aid to securing the enterprise. The main goal of the tool set is to provide a single point of administration and configuration for NT and Window 2000 systems.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Components:

Security Configuration service**:**
This service is the core engine of the tool set and runs on every Win2k system. It is responsible for the configuration and analysis and is central to the entire infrastructure.

Setup Security
This creates the initial security database (local computer policy) on a clean install of Win2k

---

Note: This is not the case for an upgraded machine, from NT or earlier. The machine may have a customized security policy and must not be overwritten. In this case, the configure option can be used to apply a configuration.

Security Configuration Editor
This is a snap in that allows the definition of computer independent security configurations, which are then saved as .inf files.

Security Configuration Manager
This is a snap in that allows the importation of saved configuration to a database. You can apply the composite information to the computer and analyze the current system configuration against the composite stored in the database.

Security Extension to Group Policy
This snap in tool extends group policy allowing the definition of the security configuration as part of the group policy object. Group policy objects can then be assigned to a specific computer or Organization Unit so that the policy can be applied to all many computers at once.

Secedit.exe
This is a command line interface to the features of the tool set.

<u>Working with the Tool set</u>

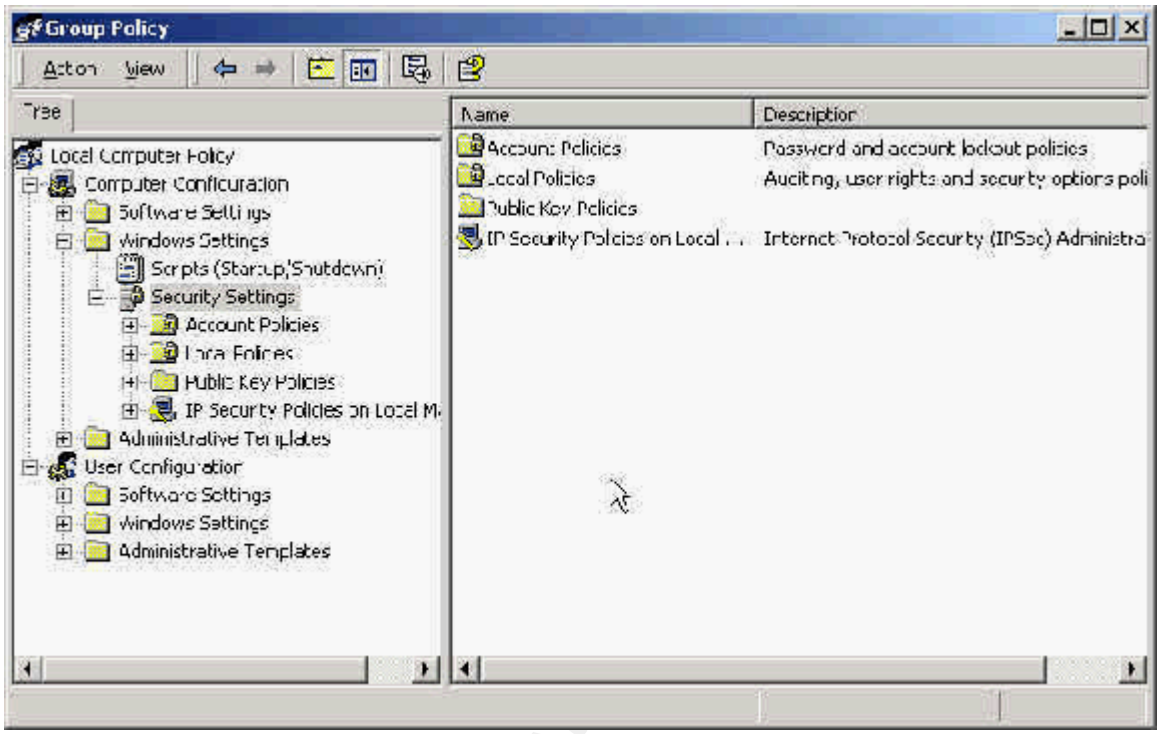
Viewing and modifying the Local Security Policy

Viewing the Local Policy

1. Log on to a workstation with *administrator* privileges.
2. To open the Croup Policy Console, click **Start, Run,** and type **gpedit.msc**. Click OK
3. Click the + next to the computer configuration, then Windows Settings, then Security Settings, then Local Policies and expand the folders.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

4. Click the security options folders under local policies.



Screenshot showing the security setting of the local machine

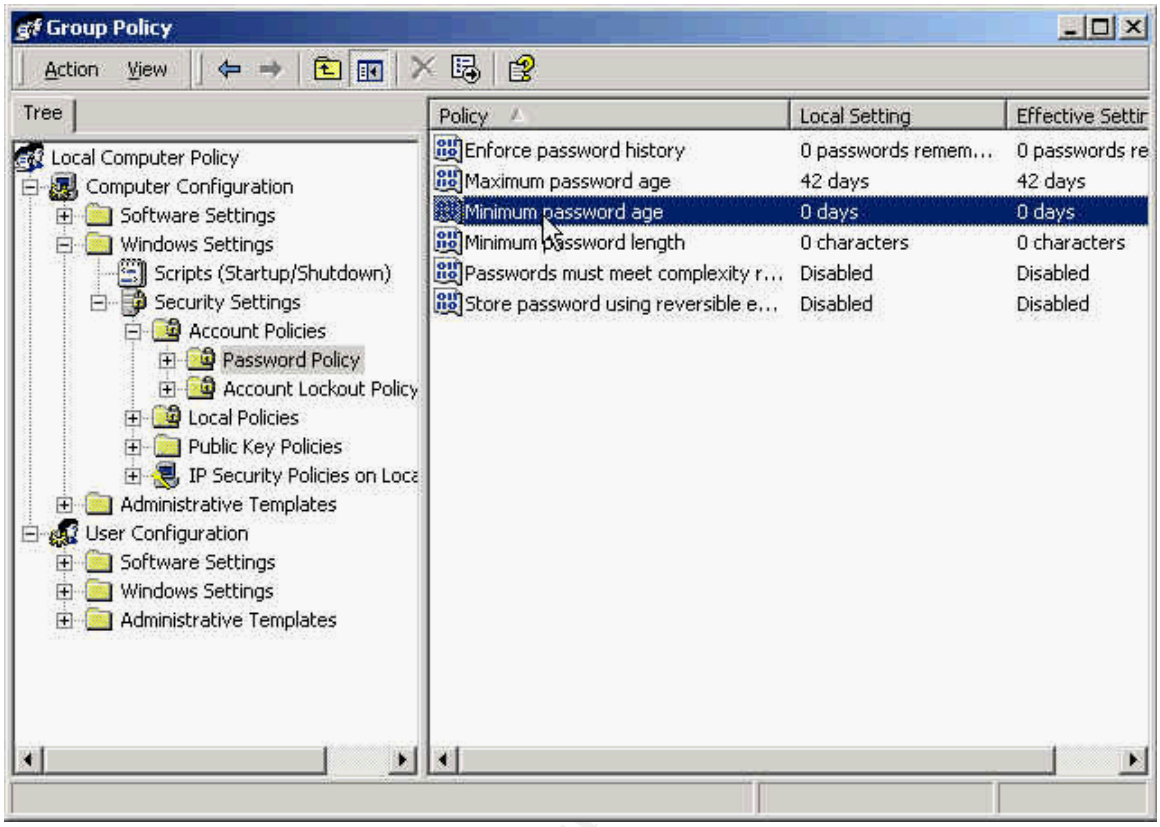
Modifying the local policy

To modify a local policy, double-click on the security item and change the desired policy. For example, to change the minimum password age,

1. Click the + next to Account Policies in the left pane
2. Click Password Policy

3. Double- click the Minimum Password Age in the right pane

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.



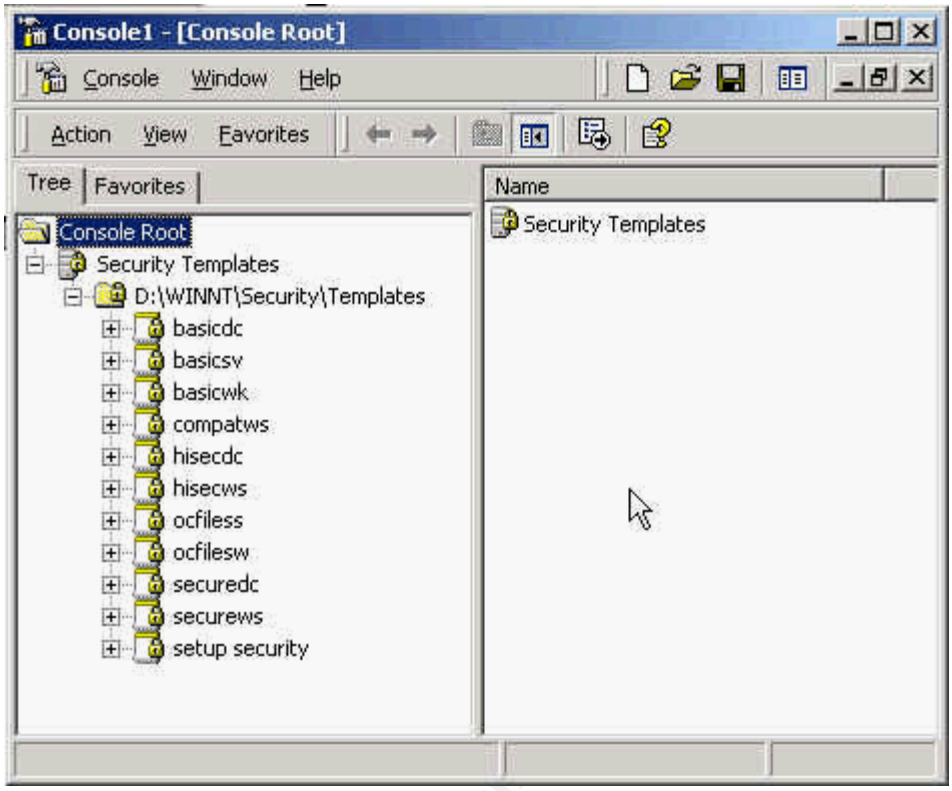
4. Set the desired minimum password age and click OK
   When you OK, the policy is then propagated through the system which causes an effective policy to be computed and applied. Status regarding the policy propagation is recorded in the event log.
5. Right click Security Settings and then click reload
   Reloading the policy updates the effective policy in the user interface

Working With Security Templates

The security templates snap in allows the creating of text-based templates that contain the settings for different scenarios and apply to many machines in the enterprise.

1. Click start, run, then type MMC and click OK
2. Click console, add\remove snap-in and click Add
3. From the list, select Security templates
4. Click ADD, the click Close
5. Click OK
6. Click the + next to security Templates to expand it
7. Click the + next to C:\Winnt\security\templates to expand it.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.



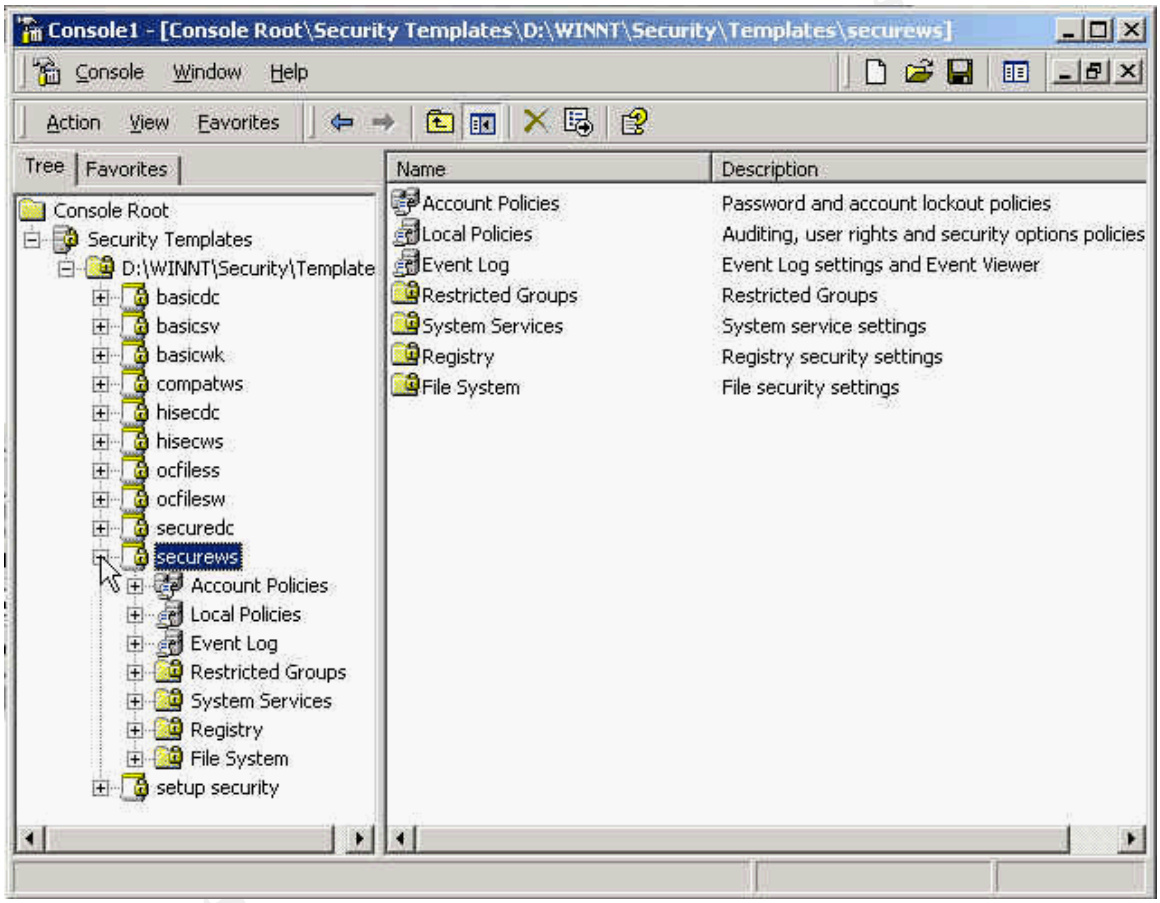
Windows 2000 ships with several predefined templates. You can create templates based on the predefined templates by right clicking the default templates and selecting SAVE AS and renaming as appropriate.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Modifying a Security Template.
In this example we will be modifying the Secure Workstation predefined template Securws.inf.

Viewing the predefined Settings.

1. In the left pane, scroll down and select the + next to Securews to expand it. Notice the setting available in the right pane.



2. Browse the policy to view the different configuration settings.

Displaying a Custom Logon Message

1. Click the Security Options node under Local Policies
2. In the right pane, scroll down and the double-click the Message Text for Users Attempting to Logon
3. Type the custom message and click OK when done.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The Security Configuration and Analysis Tool
An analysis of the security vulnerabilities on the local machine can be completed using this tool. The analysis will discover security vulnerabilities, policy discrepancies, identify changes in a system, and identify deviations from a set policy.

Using the Configuration and Analysis Tool

1. Click Start, Run, and Type MMC
2. From the console menu, select ADD\REMOVE snap-in and click Add
3. Select Security Configuration and Analysis from the list
4. Click Add, then OK

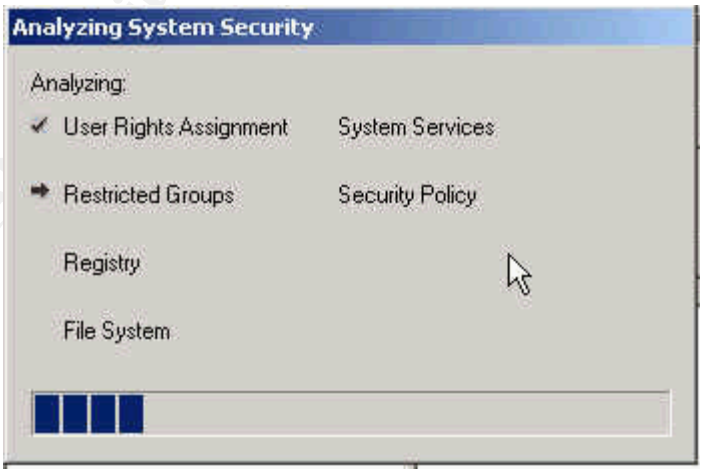
The configuration and analysis tool is database driven. Therefore a baseline database template must be created before performing an analysis.

To create the database

1. Click Security Configuration Analysis in the left pane.
2. Right click Security Configuration and Analysis in the left pane
3. Click Open Database
4. Type Mysecurews.sdb
5. Click open
6. Select Mysecure.inf
7. Click Open

Performing the Analysis

1. Right Click Security Configuration Analysis, and then select Analyze Computer Now
2. Specify the log file for the analysis operation.
3. Click open, then OK. A progress bar displays as the analysis proceeds.



Review The Results

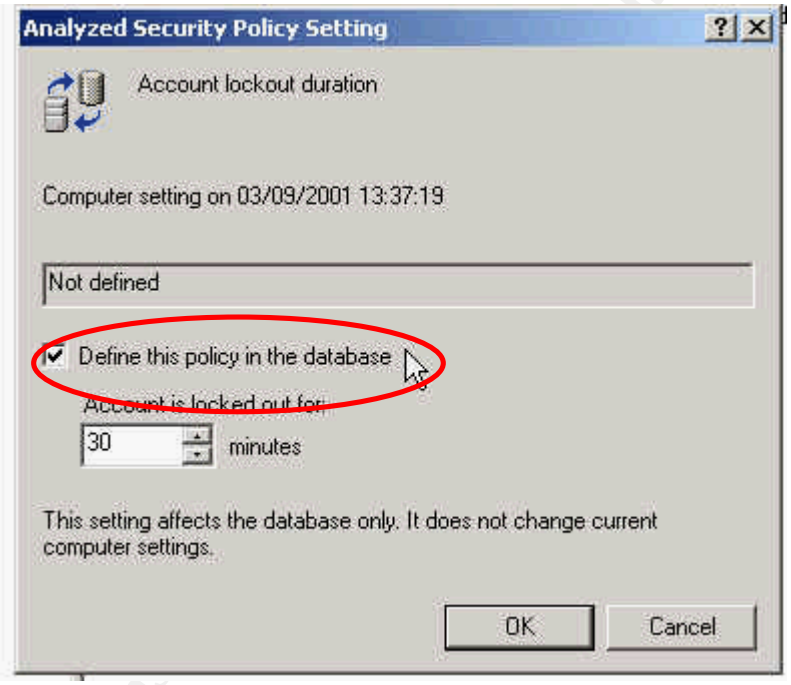
1. From the Security Configuration and Analysis node, click view
2. Select the Description bar to expose the database.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

3. Expand security Configurations & Analysis in the left pane, and then expand Local Policies and then click Security options.

In the right pane, both the database and the system settings are displayed for each object. Discrepancies are highlighted with a red flag. Consistencies are marked with a green mark. If there is no marking, then the policy has not been defined.

Relevant objects can be defined or changed by checking the Define this policy when viewing the detailed results. If this box is unchecked, the object is removed from the configurations and receives its inheritance form the parent object



Command Line Configuration and Analysis
Secedit.exe is a command line tool that can be used to automatically create and apply templates and analyze system security. The tool is useful when you have multiple computers for which a security analysis must be performed.

Secedit.exe has four areas
Analyze and Configure: Corresponds to the GUI version and has the same tasks available.
Export: Dumps the configuration into a template
Refresh Policy: Allow the triggering of policy propagation event.
Validate: Verifies the syntax of the template created using the Security snap-in.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Using Secedit.exe
Listed below are the command line syntax and switches available with Secedit.exe

To analyze system security
secedit /analyze
This command analyzes system security.

Syntax
secedit /analyze [**/DB** *filename*] [**/CFG** *filename*] [**/log** *logpath*] [**/verbose**] [**/quiet**]

Parameters
/DB *filename*
Provides the path to a database that contains the stored configuration against which the analysis will be performed. This is a required argument. If *filename* specifies a new database, the CFG *filename* argument must also be specified.

/CFG *filename*
This argument is only valid when used with the **/DB** parameter. It is the path to the security template that will be imported into the database for analysis. If this argument is not specified, the analysis is performed against any configuration already stored in the database.

/log *logpath*
The path to the log file for the process. If this is not provided, the default file is used.

/verbose
Requests more detailed progress information during the analysis.

/quiet
Suppresses screen and log output. You will still be able to view analysis results using Security Configuration and Analysis

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

To Configure system security
secedit /configure
This command configures system security by applying a stored template.
Syntax

secedit /configure [/DB *filename*] [/CFG *filename*] [/overwrite][/areas *area1 area2...*] [/log *logpath*] [/verbose] [/quiet]

Parameters

/DB *filename*
Provides the path to a database that contains the security template that should be applied. This is a required argument.

/CFG *filename*
This argument is only valid when used with the **/DB** parameter. It is the path to the security template that will be imported into the database and applied to the system. If this argument is not specified, the template already stored in the database will be applied.

/overwrite
This argument is only valid when the **/CFG** argument is also used. This specifies whether the security template in the **/CFG** argument should overwrite any template or composite template stored in the database instead of appending the results to the stored template. If this is not specified, the template in the **/CFG** argument will be appended to the stored template.

/areas *area1 area2...*
Specifies the security areas to be applied to the system. The default is "all areas." Each area should be separated by a space.

Area Name	Description
SECURITYPOLICY	Local policy and domain policy for the system, including account policies, audit policies, and so on.
GROUP_MGMT	Restricted group settings for any groups specified in the security template
USER_RIGHTS	User logon rights and granting of privileges
REGKEYS	Security on local registry keys
FILESTORE	Security on local file storage
SERVICES	Security for all defined services

/log *logpath*
Path to the log file for the process. If not specified, the default is used.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

/verbose
Specifies more detailed progress information.

/quiet
Suppresses screen

Refresh security settings
secedit /refreshpolicy
This command refreshes system security by reapplying the security settings to the Group Policy object.

Syntax

secedit /refreshpolicy {**machine_policy** | **user_policy**}[**/enforce**]

Parameters

machine_policy
Refreshes security settings for the local computer.
user_policy
Refreshes security settings for the local user account currently logged on to the computer.
/enforce
Refreshes security settings, even if there have been no changes to the Group Policy object settings.

EXPORT SECURITY SETTINGS
secedit /export
This command exports a stored template from a security database to a security template file.

Syntax

secedit /export [**/mergedPolicy**] [**/DB** *filename*] [**/CFG** *filename*] [**/areas** *area1 area 2...*] [**/log** *logPath*] [**/verbose**] [**/quiet**]

Parameters

/MergedPolicy
Merges and exports domain and local policy security settings.
/DB *filename*
Provides the path to a database that contains the template that will be exported. If a database is not provided, the system policy database is used.
/CFG *filename*

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Path and name of a file where the template should be saved.
/areas *area1 area2...*
Specifies the security areas to be exported to a template. The default is "all areas." Each area should be separated by a space.

Area Name	Description
SECURITYPOLICY	Local policy and domain policy for the system, including account policies, audit policies, and so on.
GROUP_MGMT	Restricted group settings for any groups specified in the security template
USER_RIGHTS	User logon rights and granting of privileges
REGKEYS	Security on local registry keys
FILESTORE	Security on local file storage
SERVICES	Security for all defined services

/log *logpath*
Path to the log file for the process. If not specified, the default is used.

/verbose
Specifies more detailed progress information.

/quiet
Suppresses screen and log output

VALIDATE A SECURITY CONFIGURATION FILE

secedit /validate
This command validates the syntax of a security template you want to import into a database for analysis or application to a system.

Syntax

secedit /validate *filename*

© SANS Institute 2003, Author retains full rights.

Tool: Encrypted File System (EFS)
Location: Installed as part of the operating system

Encrypting local file and folders is accomplished through a technology called Encrypted File System. It is included with the windows 2000 operating system and is based on public – key encryption and takes advantage of the Crypto API architecture. Each file is encrypted using a randomly generated file encryption key, which is independent of a user's public/private key pair.

Files are automatically encrypted to a third party, called a recovery agent. In the event of a key loss, the recovery agent can decrypt the files. The bulk of the file is encrypted with a single symmetric key. The symmetric key is then encrypted twice: once with the users public key and once with the recovery agent's public key to allow decryption.

Note: EFS supports encryption and decryption of files stored on local drives as well as files stored on remote servers. In the case of remote servers, you can encrypt files and folders on the server but the data is not protected over the wire. An encryption protocol such as IPSec is needed to encrypt data over the wire.

Using Encrypting File System
The default configuration of EFS allows users to encrypt files without administrator action. EFS automatically generate a public\private key pair and file encryption certificate for the file encryption for a user the first time the file is encrypted.

File encryption is supported on a per file or for an entire folder. Encrypting folders is transparently enforced. Each file has a unique key making it safe to rename. If you copy an unencrypted file into an encrypted folder, the file remains unencrypted.

Data Recovery
With file encryption you run the risk of being unable to decrypt the file. EFS provides built in data recovery support. The Window 2000 security infrastructure enforces the configuration of data recovery keys. EFS allows the recovery agent to recover encrypted data if the users leaves the company. Only the file encryption key is available, not the user's private key. This ensures private information is only revealed to the recovery agent.

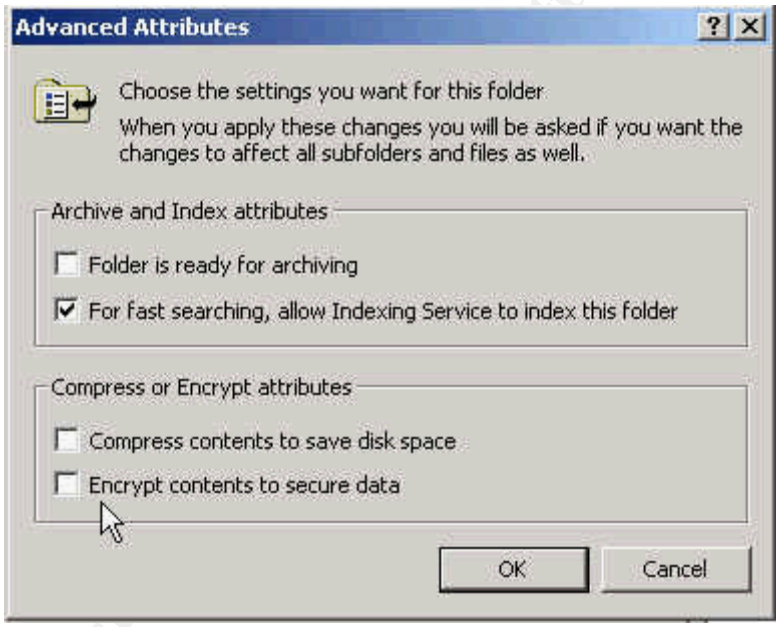
Note: Protecting the recovery agent key is critical. Use the recovery agent to export the key to a floppy and safeguard the floppy in a safe or other secure area. The recovery key should be deleted from the server once the export has been made.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Using EFS

Windows Explorer
Encrypting:

1. Click Start, click programs, click Accessories, click Windows Explorer
2. Rich click the folder or file name that you wish to encrypt and select properties
3. On the general tab



4. On the Advanced Attributes dialog box, select Encrypt content to secure data, then click OK.
5. Click OK
6. Your are then asked if you wish to encrypt the file or just the folder. If the folder is empty, choose to encrypt the folder only.
7. A dialog box will then show the progress of the encryption.

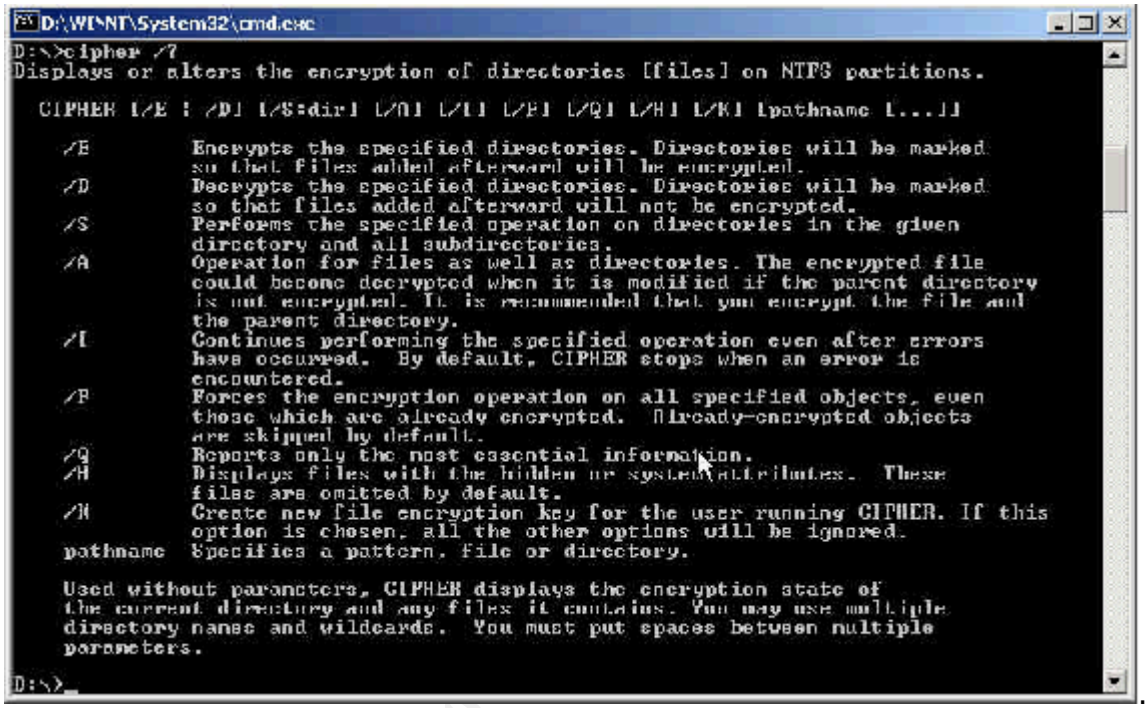
Decrypting

1. Open Windows Explorer
2. Right click the file or folder
3. On the general tab of the properties, click advanced
4. On the advanced attributes, clear the check box and click OK

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Using CIPHER.EXE
Cypher.exe is a command line to tool the provide much of the same functionality of the GUI interface.

Below is a screen shot of the command line switches available to the tool.



Encrypting with Cipher.exe

To use the **cipher** command to encrypt a file or folder, type the following command:

C:\>cipher **/e** /s:"c:\foldername\file"

To decrypt the folder or file, just apply a /d switch.

C:\>cipher **/d** /s:"c:\foldername\file"

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Using Encrypted Files or Folders

Using encrypted files and folder is seamless to the end user. All the encryption and decryption is done in the background when opening and closing the file. The end user who encrypted the file or folder will not notice anything different and files will open as before. Only the user who encrypted the file can decrypt and make it available for others.

Copying and moving files works just as works just as all NTFS file permissions when moving and copying files and folders. Backing and restoring encrypted files is also just as before, however, the back up software should support windows 2000 features to ensure the encrypted file is not lost.

The following describes the limitations for copying encrypted files and folders:

- **To copy a file or folder on the same computer from one NTFS partition in a Windows 2000 location to another NTFS partition in a Windows 2000 location**. Copy the file or folder as you would an unencrypted file. Use Windows Explorer or the command prompt. The copy is encrypted.
- **To copy a file or folder on the same computer from an NTFS partition in a Windows 2000 volume to a FAT partition**. Copy the file or folder as you would an unencrypted file. Use Windows Explorer or the command prompt. Because the destination file system does not support encryption, the copy is in clear text.
- **To copy a file or folder to a different computer where both use the NTFS partitions in Windows 2000**. Copy the file or folder as you would an unencrypted file. Use Windows Explorer or the command prompt. If the remote computer allows you to encrypt files, the copy is encrypted; otherwise it is in clear text. Note that the remote computer must be trusted for delegation; in a domain environment, remote encryption is not enabled by default.
- **To copy a file or folder to a different computer from an NTFS partition in a Windows 2000 location to a FAT or NTFS in a Windows NT® 4.0 location**. Copy the file or folder as you would an unencrypted file. Use Windows Explorer or the command prompt. Because the destination file system does not support encryption, the copy is in clear text

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Tool: Internet Protocol Security (IPSec)
Location: Installed with the operating system

Designed by the IETF, IPSec supports network level authentication, data integrity and encryption. The windows 2000 implementation builds on the IETF architecture by integrating it into active directory. This provides a great deal of control over how IPSec is implemented in the enterprise.

Win2K IPSec incorporates several encryption algorithms including Diffie-Hellman Technique, HMAC, HMAC-MD5, and HMAC-SHA & DES-CBS. It also is flexible with the security protocols with the integration of Internet Security Association and Key Management Protocol, Oakley Key Determination, IP Authentication and IP Encapsulating Protocol.

Note: An explanation of how the different algorithms work-

Diffie-Hellman (DH) Technique -The Diffie-Hellman Technique is a public key cryptography algorithm that allows two communicating entities to agree on a shared key.

Hash Message Authentication Code (HMAC) - HMAC is a secret-key algorithm providing integrity and authentication. Authentication using keyed hash produces a digital signature for the packet that can be verified by the receiver. If the message changes in transit, the hash value is different and the IP packet is rejected.

HMAC-MD5 - Message Digest function 95 (MD5) is a hash function that produces a 128-bit value.

HMAC-SHA - Secure Hash Algorithm (SHA) is a hash function that produces a 160-bit value.

DES-CBC Data Encryption Standard (DES)—Cipher block chaining (CBC) is a secret key algorithm used for confidentiality. A random number is generated and used with the secret key to encrypt the data.

Secure Servers
IPSec for all unicast traffic is either *requested but optional* or *requested and required*, depending on the configuration of the server. Clients need only a default policy to respond to security requests from the server. Once IPSec connections have been established, the policy remains in effect for one hour after the last packet is sent. This allows time for the client to clean up the security associations and return to the respond only state. This is the easiest approach to take, however, the first packets sent should not contain sensitive data to allow

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

time for IPSec to setup. This configuration is appropriate for INTERNAL SERVERS ONLY because the server is allowing incoming, clear text, unsecured packets. For Internet accessible servers, the client must receive an IPSec policy so that it requests IPSec security for traffic when it attempts to send data to the server.

Configuring an IPSec Policy

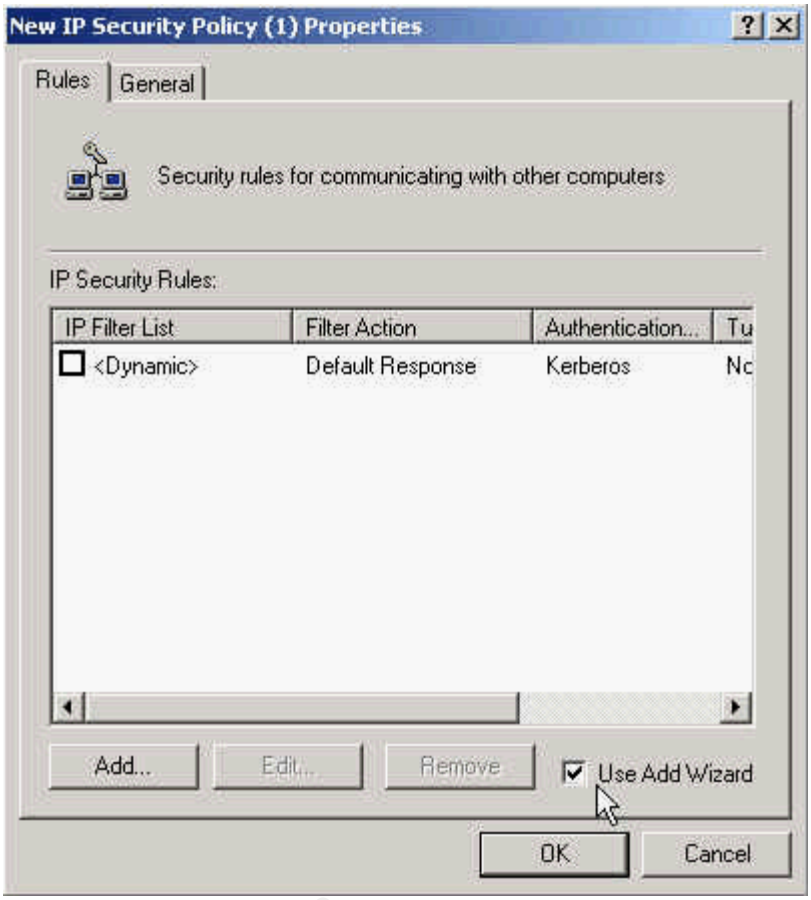
To configure an IPSec policy, open the MMC console and add the IPSec Security Policy Snap-in.

Before configuring the IPSec Authentication Method, Filter List, or Negotiation method, you must first create a new policy.

To create an IPSec Policy

1. Right-click **IP Security Policies on Local Machine**, and then click **Create IP Security Policy**. The IP Security Policy Wizard appears.
2. Click **Next**
3. Type a descriptive name for the policy and click **next**.
4. Clear the **Activate the default response rule** check box, and then click **Next**
5. Check the **Edit Properties** (it is checked by default), and then click **Finish**.
6. In the properties dialog box for the policy you just created, ensure that the Use Add Wizard check box is selected.

© SANS Institute 2003, Author retains full rights



© SANS Institute 2003,

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

7. Click ADD to start the security rule wizard, click next.
8. Add the IP address of the tunnel end point, click next
9. Select the network type
10. Choose the authentication method

© SANS Institute 2003, Author retains full rights

Tool: Kerberos Encryption Protocol
Location: Installed with the operating system

The Kerberos protocol is a standard that addresses network authentication and identity verification. It does not address authorization. The Windows 2000 implementation of Kerberos v5 protocol is designed for interoperability with other security services based in the MIT implementation of Kerberos.

An individual Kerberos deployment is referred to as a realm and is analogous to a Windows domain. The realm consists of a Key Distribution Center (KDC) and applications and services that use the Kerberos authentication protocol. Similar to a Windows domain, security principals belong to a realm and are known throughout that realm.

Components
Kerberos is made up of several components that work together to provide the total solution.

Credential Cache
The Credential Cache is used by Kerberos to store authentication information. Once authenticated to a Kerberos realm, tickets obtained are stored in the cache to that they can be reused during the lifetime of the ticket.

Kinit
The kinit utility logs in to the Kerberos realm using the client's key that is derived from the users password. The Kerberos client then receives a Ticket Granting Ticket (TGT) as confirmation of successful authentication

Klist
A utility to view the tickets in the credential cache.

Kdestroy
Kdestroy is used to destroy tickets when the services or applications are finished with the tickets. Often implemented as part of a logout procedure.

Kpasswd
A utility used by Kerberos to change password for a given identity. This utility is not defined by the Kerberos standard and, therefore implementation will vary.

Kerberos Key Distribution Center (KDC)
The KDC is a network service that accepts requests for tickets from kerberos clients, validates their identity, and grants tickets to them. A typical installation will include a master KDC with a series of slaves to support the network requirements.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Key Database (KDB)
This data hold the account information for the network users and resources. The KDC uses this database to verify the identities in a distributed environment.

Kadmin
This is a utility used by the administrator to update account entries in the KDB. Changes are done only at the master KDC using the local Kadmin tool or vie the Kadmin service.

Kprop
This is system utility that synchronizes the master KDB with the slaves.

Using Kerberos

There are many scenarios to implement the Kerberos technology in a windows 2000 domain. The three main parts to keep in mind when developing a solution are the Kerberos Client, Kerberos, KDC, and the available network resources.

As far as the implementation, there are four fundamental implementation approaches that address the multiple scenarios derived from the variable above. The table below shows the permutations of the variables.

	Access to Windows 2000 Resources	Access to Non-Windows 2000 Resources
Windows 2000Client Authentication to Windows KDC	Native	One-way Trust or Service Account
Windows 2000 Client Authentication to Non-Windows KDC	Two-way Trust	Client Configuration
Non-Windows Client Authentication to Non-Windows KDC	Two-way Trust	Native
Non-Windows Client Authentication to Windows KDC	Client Configuration	One-way Trust or Service Account

Native

Native refers to scenarios using matched set of Kerberos technology. Usually Windows 2000 based clients authenticating to windows 2000 based KDC and accessing windows 2000 based resources. There are really no interoperability challenges and therefore no additional implementation or configuration is needed. For example, Windows 2000 automatically uses Kerberos authentication upon the first logon.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

One Way Trust

This refers to creating a relationship of trust between a domain and a realm that tickets generated in one realm will be recognized and accepted. For example, a one-way trust could exist from a Kerberos realm to a windows 2000 domain and would allow users to logon.

Service Account

Windows 2000 also support non-windows Kerberos services in the windows domain. The services are represented as a "service account". In this manner Unix client can be made accessible to Kerberos clients

Account Mapping

To allow for policy and authorization, the Kerberos realm account must have a Windows 2000 account mapped to it. This mapping is contained in the AltSecurityId property of each Windows 2000 account. The mappings can be a one-to-one or a one-to-many mapping. A one to one mapping is recommended to allow for maximum administrative flexibility.

Synchronizing Accounts

Because Kerberos exists in many implementations and on many platforms, there is no one single way to synchronize the active directory accounts with the Kerberos realm accounts. The primary interfaces are active directory ADSI and LDAP. The 3 primary methods of synchronization are the modification of the Kprop, modification of Kadmin or using a batch file to call Kadmin.

The modification of the Kprop service is accomplished by creating a Kpropd on a DC in the windows 2000 domain. A kpropd, or Kprop *daemon,* is a server that accepts connection from the Kprop service. The kpropd will run as a trusted member of the Kprop service for the Kerberos security realm. When kprop receives an update, the changes are applied via the secure update package to the active directory. Kpropd receives a KD dump file of all the security principals in the realm. Kpropd then uses this file to create, delete and update account information.

The Kadmin utility if the utility used for Kerberos realm administration. Functionality can be added to the windows 2000 domain and has the advantage of a familiar interface for Kerberos realm administrators. Synchronization is accomplished by a *synch all* operation and initializes the Windows 2000 domain with a list of all users by calling the secure update package for each user in the database.

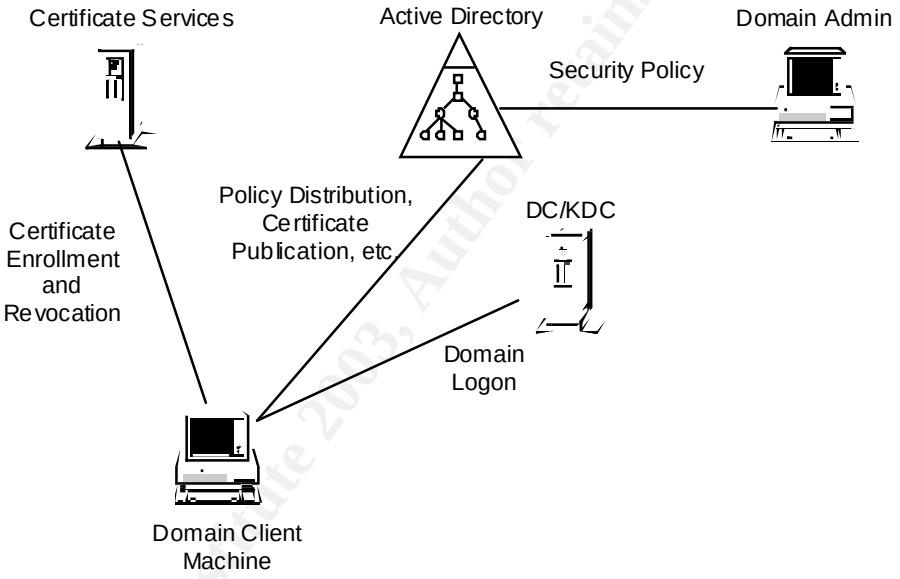
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Tool: Public Key Infrastructure
Location: Support and Services Installed with the operating system

Public Key Infrastructure (PKI), as the name suggests, is a framework by which systems can be made secure. Its main purpose is to provide business the services to use public key cryptography. Public key cryptography is crucial for e-commerce, applications and other services that require distributed security.

COMPONENTS

The figure below represents the components of PKI. This is a logical view and many functions can be run from a single server. The key element is the certificate services, which allows the deployment of more than one CA. The CA's support issuance and revocation and is integrated with active directory.

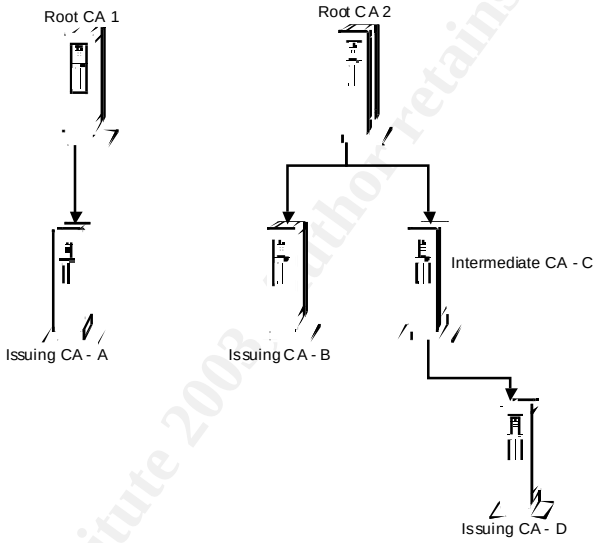


PKI works in conjunction with the Kerberos Key Distribution Center and provides enhancements to allow applications to scale and address extranet issues.

© SANS Institute 2003, Author retains full rights.

The Windows 2000 PKI assumes a hierarchical CA model. The CA hierarchy consists of a root CA and several clearly defined children CA's. The subordinate CA's are usually referred to as intermediate or issuing CA's. The main advantage to this model is that verification of certificates requires trust in only a relatively small number of root CA's while supporting the flexibility in the number of issuing CA's. The reason for supporting multiple issuing CA's are

- Usage – Certificates may be issued for a number of purposes. The issuing policy for these may be distinct and the separation provide the basis for administration of these policies
- Organizational divisions
- Geographic divisions



© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Certificate Authorities

Deploying enterprise CA is a straightforward operation. It is recommended that you establish a domain prior to creating the CA. Then establish the root CA.

The root CA can run on any windows 2000 server including the domain controller. Factors such as physical security, connectivity should be considered. The CA names are bound to their certificates and hence cannot be changed. Consider the CA carefully. Key generation is done during the installation and is unique to each CA. The installation process also generates a self-signed certificate, using the CA's public/private key pair. Information concerning the CA is written into a CA object in Active directory. The CA setup also automatically installs and configures the enterprise Policy module. The administrator can then modify the policy module as needed.

The CA is a highly attractive target all reasonable security precautions should be taken to protect this root server and the CA keys.

Trusts

In order for PKI to work, trust relationships must be dealt with across multiple CA hierarchies. This could involve private and commercial, such as Versign, CA's. Trusts in root CA's may be set by group policy to establish trust relationships used by domain clients in verifying PK certificates. The administrator also establishes usage requirements associated with the CA. Restrictions are specified based on the object identifiers (OID). This provides a means to restricting use of any of the following areas.

- Server authentication
- Client authentication
- Code signing
- E-mail
- IPSec end system
- IPSec tunnel
- IPSec user
- Time stamping
- EFS

Certificate Enrollment and Renewal

Certificate enrollment is controlled by to key elements: certificate types and auto-enrollment objects. These are integrated with group policy and may be defined on a site, domain, OU, computer or user bases.

Certificate types provide a template for a certificate and associate it wit a common name for ease of administration. The template defines the naming requirements, validity period, allowable CSP's for private key generation, algorithms, and extensions that should be incorporated into the certificate. The

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Certificate type is logically separated into computer and user types and applied to the policy objects. Once defined, the certificate types are available for use with the auto-enrollment objects.

The auto-enrollment object defines the policy for the certificates that an entity in the domain should have. The object provides information to determine whether an entity has the required certificates and to enroll for those certificates with missing enterprise CA's and define policy on certificate renewal.

Use of PKI

The use of PKI will vary depending on the application and resources that need to be secured. This section provides some typical scenario's that currently take advantage of PKI

Web Security

The Internet is fast becoming the choice for deploying solutions and naturally, security is a high priority for these sites. The main considerations for securing websites are:

- Server authentication – enable clients to verify the servers that they are connected with.
- Client Authentication – to allow servers to verify the clients' identity.
- Confidentiality – Encryption of data between clients and server to prevent it exposure over public Internet links.

SSL and TLS (transport Layer Security both use PK based security key negotiation to generate unique encryption key for each client server session. They are most commonly associated with the HPPS protocol.

Using SSL and TLS requires both client and server to have certificates issued by a mutually trusted CA, allowing the parties to authenticate each other. In this mode, certificates are exchanged along with the data. Each side can then validate the certificate and verify the possession of the private key. The identifying information included in the certificate can then be used to make additional access control decisions such as which data the client can access.

Once the client and the server have authenticated, they can begin to negotiate a secure session and session key. Use of mutual authentication is recommended in the enterprise environment because it allows the use of windows based access control mechanisms.

Email Security

© SANS Institute 2003, Author retains full rights

Security for e-mail has been available for several years now and is widely deployed. These systems rely on PKI for Digital signatures and bulk encryption. The distributed nature of e-mail has been the main reason for the use of PKI.

The operation of these systems requires the use of a user's private key to digitally sign the outgoing message. The certificate is sent with the message to verify the signature. Once the certificate is verified, the user can use the contained public key to decrypt the message.

Smart Card Logon

Windows 2000 supports the use of smart card logon as a secure alternative to domain authentication. This relies on a PC/SC workgroup compliant smart card and RSA capable smart card supporting CryptoAPI CSP's. This method makes use of the PKINIT protocol to integrate PK based authentication with the Windows 2000 ACL.

When logging on the system recognizes a smart card insertion event as an alternative to the CTRL-ALT-DEL to initiate a logon. The user is then prompted for a PIN, which controls access to operations with the private key stored on the card.

© SANS Institute 2003, Author retains full rights

References

Crawford, Russel. Windows 2000 Administration, Redmond: Microsoft Press, 2000. 629-641

Fossen, Jason. Windows 2000:PKI, GIAC Workbook Version 3.0 Sans Institute, 2000

Norberg, Stefan. Securing Windows NT/2000 Servers for the Internet, O'Reilly, January 2001. 87-101

Microsoft, "Public Key Infrastructure." White Paper, Redmond: Microsoft, 1999

Microsoft, "Windows 2000 Kerberos Authentication." White Paper, Redmond: Microsoft, 1999

Microsoft, Microsoft TechNet: Technical Information CD (TechNet): January 2001. Volume 9, Issue 1, Redmond, Microsoft 2001.

All screen captures in this document were made with Snag-It 32 v 5.01 which can be obtained at:

http://www.techsmith.com/products/snagit/default.asp

© SANS Institute 2003, Author retains full rights.

Last Updated: June 20th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**