4.1. Group Design

The following table shows the recommended approaches to managing users, groups, and permissions.

Strategy	Use	Description	Application
UGLR	Used in mixed mode domains and in native mode domains (does not use universal groups, which are also not available in mixed mode).	**U**: Place **U**ser Accounts **G**: Into **G**lobal groups **L**: Into Domain **L**ocal groups **R**: Assign Permissions to domain local groups to give access to **R**esources	1. Identify the users in the domain who use the same resources and perform the same tasks. Group these accounts together in global groups. 2. Create new domain local groups if necessary, or use the built-in groups to control access to resources. 3. Combine all global groups that need access to the same resources into the domain local group that controls those resources. 4. Assign permissions to the resources to the domain local group.
(J)UGULR	Used in native mode domains, when there is more than one domain, and you need to grant access to similar groups defined in multiple domains.	**U**: Place **U**ser Accounts **G**: Into **G**lobal groups **U**: Into **U**niversal groups **L**: Into Domain **L**ocal groups **R**: Assign	Universal groups should be used when you need to grant access to similar groups defined in multiple domains. It is best to add global groups to universal groups, instead of placing user accounts directly in universal groups.

		Permissions to domain local groups to give access to **R**esources	

To keep the number of groups to a minimum, you should *not* automatically use universal groups, even though they might be supported.

- Use universal groups only if both the users and the resources are located in *multiple* domains.
- You would *not* need universal groups in a single-domain design.
- You would *not* need universal groups if the resources you were controlling access to were located in a single domain.

© Sergey Gorokhod
MCT/MCSE/MCITP/MCTS/MCSA/CCSE/CCSA/CCNA/A+®
E-mail: sergey@infosec.co.il
Mob: (+972) 526848757

4.2. Restricted Group

Restricted Group policies allow you to control group memberships using Group Policy. With Restricted Groups, you can ensure that group membership is not changed. Keep in mind the following when using Restricted Groups:

- Restricted Groups is used primarily to configure local group membership for workstations and member servers.
- You can use Restricted Groups to define group members as well as groups to which the defined group belongs (a.k.a. **Member of**).
- When the policy is applied:
    - Any members not specified in the policy as allowed group members are removed.
    - Any member not currently a member of the group is added.
    - The group is added to groups specified in the **Member of** list. **Note:** Configuring **Member of** settings will not remove additional existing members from the target group. Also, the Restricted Group may also be a member of other groups not defined by the **Member of** list.
- As a best practice, use Restricted Groups to add or remove members, or use them to define **Member of** relationships. Do not use both as this could lead to unpredictable effects in group memberships.
- To prevent any user from becoming a member of a specific group, define the Restricted Group with no members.
- When defining Restricted Groups, some groups must have at least the Administrator as a member. In this case, you will not be able to save your changes until Administrator is added to the list of members.
- If a specific group is identified in multiple GPOs at different level, only the group membership identified in the last-applied GPO will be in effect. In other words, group membership is not merged or combined.

4.3. Access Control Design

Windows uses Access Control Lists (ACLs) to control access to resources such as files, printers, and Active Directory objects. Users or groups are added to the ACL of an object and then assigned permissions. The permissions identify the actions that can be performed on that object.

Be aware of the following concepts about working with ACLs that are common for most object types:

- Explicit permissions are defined when a user or group is added to the ACL and assigned permissions.
- Permissions assigned to parent objects (such as folders) are inherited to the objects within the parent object (such as files or folders). If desired, you can disable permission inheritance.
- Permissions granted to a group are received by all group members.
- Permissions are cumulative. Users have the sum of permissions granted to the user, to any groups of which the user is a member, and permissions received through inheritance.
- Deny permissions override Allow permissions.
- Whenever possible, assign permissions to groups rather than to individual users.
- To assign permissions to all users, assign permissions to the Authenticated Users group instead of Everyone.

The following table summarizes considerations for designing ACLs for various objects.

Resource Type	Considerations
File System	File system access can be controlled by two sets of permissions: share permissions and NTFS permissions. Be aware of the following considerations for implementing file system access control: • NTFS permissions can only be set on NTFS partitions. Share permissions can be configured for both FAT and NTFS partitions.

	• Share permissions apply only to files accessed through a network connection. NTFS permissions apply to both local and remote access. • You can configure NTFS permissions through Group Policy. • For NTFS files, each file has an owner. The owner can modify the access control list. If you are unable to modify NTFS permissions, take ownership of the file. • Users must have the Read permission to back up a file. They need the Read and Write permissions to restore files. • The Backup Operators group has user rights that allow group members to back up and restore files. You can divide the backup and restore responsibilities by assigning the appropriate user rights to custom groups. • To troubleshoot NTFS permissions, you can view the effective permissions that a user has to a folder or a file. • For extra control over NTFS permissions, edit the Advanced permissions.
Printers	Printers have a small set of permissions that can be assigned. Be aware of the following when managing printer permissions: • By default, the print job owner (the user who printed the document) can manage the document in the print queue. • To allow a user to manage all documents in the print queue, assign the Manage Documents permission. • Grant the Manage Printers permission to allow a user to start and stop the print server.
Active Directory objects	Permissions set on Active Directory objects define the operations that users can perform on that object. Be aware of the following considerations: • By default, permissions granted to the domain or the OU are inherited to all objects within and below the parent container. • You can take advantage of inheritance by structuring Active Directory so that OUs represent administrative boundaries. All

	objects within the OU have the same administrative requirements. • Although you can configure permissions on individual objects, assign permissions to the parent container whenever possible. • Use the Delegation of Control wizard to assign Active Directory permissions. Using the wizard, you identify the users and the groups and define the actions they will be allowed to perform (such as changing passwords on user accounts).
Registry	Each registry key has an ACL that can be used to control access to the key. Be aware of the following when designing registry permissions: • Like file system and Active Directory permissions, permissions set higher up in the registry are inherited to child keys and sub-keys. • File system permissions set on the registry files control access to the registry, but do not affect the ability to edit individual keys. You should not modify file system permissions set on registry files. • You can use Group Policy to configure registry permissions. • By default, remote editing of the registry (such as through an MMC snap-in) is enabled. o Remote access is enabled through the Remote Registry Service service. This service is required by domain controllers for Active Directory replication and by the Spooler service when accessing a remote printer. Disabling this service can render other necessary services inoperable. o Permissions to remotely edit the registry are configured by setting permissions on the **WinReg** key (located at HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\). o By default, Administrators have Full Control to this key. To allow other users remote registry access, edit the permissions on the **WinReg** key.

	• You can configure auditing for the registry by enabling Object Access auditing and then defining the events to audit on individual registry keys.
System Services	You can configure permissions on services to control which users can start, stop, or modify service settings. • You can control the startup behavior and configure permissions on services using Group Policy. • There is no inheritance when configuring service permissions. Permissions must be configured on each individual service.

4.4. EFS Design

You can protect the confidentiality of files by allowing users to use the Encrypted File System (EFS). Designing for EFS involves the following design tasks:

- Choosing whether to allow EFS.
- Choosing the certificate type to use.
- Designing the file recovery mechanism.
- Designing for remote encryption.

Choosing to Allow EFS

The use of EFS takes planning to ensure that authorized users can access encrypted files, that files can be properly recovered if necessary, and that only authorized users have access to encrypted files. Many organizations decide to disable EFS completely until a well-designed solution can be put into place.

- By default, EFS is enabled for all users.
- You can use Group Policy to disable EFS for a domain.
- You can also allow EFS through Group Policy for only specific users.
- To enforce more secure encryption, enable the **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing** policy. This policy enforces 3DES with 128-bit encryption.

Choosing the Certificate Type

EFS uses certificates to encrypt files and to enable file recovery. When designing an EFS solution, you need to choose the type of certificates that will be used for encryption.

Method	Description
Self-signed	A self-signed certificate is one that is automatically generated when needed. With self-signed certificates, • A Public Key Infrastructure (PKI) is not required. • Certificates are generated automatically when needed. • Recovery agents and user certificates are difficult to track.

	• Centralized key archival and recovery is not possible. Users will be less likely to back up private keys, making file recovery difficult if not impossible. Self-signed certificates are typically used in small networks or for non-domain members.
Public Key Infrastructure (PKI)	For large deployments, you should configure a Public Key Infrastructure (PKI) to distribute certificates to both users and data recovery agents. A PKI offers the following advantages: • You can configure autoenrollment using certificate templates. • Certificates are stored in Active Directory and are available to users automatically regardless of the computer they use. • You can configure automatic key archival. • You can easily designate data recovery agents for portions of the network through Group Policy.

Designing File Recovery

Just like you must design and test a file restore mechanism to go along with your regular backups, you must identify how encrypted files are to be recovered. There are two approaches to recovering encrypted files:

Method	Description
Key Recovery	With key recovery, you recover encrypted files by restoring user's private keys. Be aware of the following issues: • Archive user's private keys. When using a 2003 PKI, you can configure automatic key archival. • To recover lost files, restore the user's private key to the local system. Have the user log on to open the file. • Protect the private keys to keep them from being accessed by unauthorized users. Allow only authorized users to restore archived keys.

	• You can disable all data recovery agents (DRAs) to restrict access only to the authorized users.
File Recovery	With file recovery, you designate one or more data recovery agents (DRAs) who can recover encrypted files. Be aware of the following issues: • By default, the domain Administrator account is the recovery agent for the domain. The local Administrator user account is the default recovery agent in a workgroup. • You can use Group Policy to identify DRAs for the domain or over specific OUs. • DRAs must be designated before files are encrypted. Because the DRA can open and read all encrypted files, you should put strict controls in place to limit accessibility to file recovery capabilities. Consider the following recommendations: • Establish a written policy that identifies the circumstances when file recovery is allowed. • Give DRAs special user accounts that are only used for file recovery. • Configure offline workstations that are only used for file recovery. • Export DRA private keys and keep them in a secure location. Allow access to the private keys only for file recovery. • When file recovery is necessary, import the DRA's private key to the recovery workstation. Recover the necessary file(s), then delete the private key from the workstation.

Designing Remote Encryption

With EFS, users can only save encrypted files to their local computers. If you want to allow users to store encrypted files on a network location, you must design for remote encryption. There are two methods for enabling and securing remote encryption.

Method	Description

Delegated server mode	With delegated server mode, users save encrypted files on a network server. The following conditions must be met to be able to save files on a network server:
	
	• The server must be trusted for delegation. Enable this setting on the properties of the computer account.
	• The user account must be enabled for delegation. Enable this setting in the user account properties.
	• The destination share must be on an NTFS partition.
	• The server and the user must be in the same forest.
	• Smart card certificates cannot be used for encryption.
	• The server must have access to a copy of the user certificate. This can be done by:
	  o Storing the certificates in Active Directory.
	  o Having the user log on interactively to the server.
	  o Configuring a roaming user profile for the user.
	  o Copying the certificate to the server manually.
	
	Note: *When encrypted files are copied to a network server, the file is decrypted before being sent on the network, then encrypted by the server before saving. To protect the file while it is being copied to the server, force the server to require IPSec.*

EFS over WebDAV	You can use WebDAV folders on an IIS server to store encrypted files. When using EFS with WebDAV: • Files sent to the WebDAV folder are sent in their encrypted form. For this reason, encrypted files are protected as they are sent without deploying an additional mechanism such as SSL or IPSec. • Files have a 400 MB size limitation. • Files can be saved on an IIS server that is not in the same forest as the source computer.

Note: *In addition to protecting files as they are sent across the network, you should also consider whether unencrypted copies of files are available on the local system.*

- To enforce encryption, set encryption on the parent folder and require that all sensitive files are saved to the folder and not to other locations.
- Some programs save temporary copies of data. To ensure that data is never saved in an unencrypted format, encrypt the folder where temporary data is stored.

© Sergey Gorokhod
MCT/MCSE/MCITP/MCTS/MCSA/CCSE/CCSA/CCNA/A+®
E-mail: sergey@infosec.co.il
Mob: (+972) 526848757

4.5. Auditing

General auditing characteristics are configured through audit policies. Audit policies are stored in either the domain or local Group Policy. An audit policy is either enabled or disabled. When it is enabled, you must specify what type of events to log.

- Audit Success to identify who has gained access and to verify that people should do all they are doing.
- Audit Failure to identify patterns of attempted access.

The following table describes the nine audit policies configurable through Group Policy.

This Policy...	Audits These Actions
Account Logon	• An account is authenticated. • Recorded by the local computer for the local account. • Recorded by domain controller for the Active Directory account.
Account Management	Actions on user accounts and groups, including: • Create • Rename • Disable/enable • Delete • Change the password
Directory Service Access	Access to an Active Directory object. ***Note:*** *You must configure auditing on the specific objects you want to track.*
Logon	• Logon/off to/from the local system. • A network connection made or disconnected. • Recorded on the computer in addition to account logon events.

Object Access	A file, folder, or printer is accessed. Can also be used to audit actions taken by a certificate authority or access to specific registry or IIS metabase settings. ***Note:*** *You must configure auditing on the specific objects you want to track.*
Policy Change	Changes made to password or account logon settings, user rights, or audit policies.
Privilege Use	• A user exercises a user right. • An administrator takes ownership of an object.
Process Tracking	An application performs an action (this is used mainly for program debugging and tracking).
System	• The system is restarted or shut down. • An event affects security or the Security log.

Note: *With both Directory Service Access and Object Access auditing, configuring auditing requires two steps:*

1. *Enable auditing in the local security policy or Group Policy.*
2. *Configure auditing on the specific objects. For example, you might edit the System Access Control List (SACL) of the Active Directory object or the NTFS file or folder to identify the users or groups and the actions to track. For CA auditing, identify the specific CA actions to track in the CA properties.*

© Sergey Gorokhod
MCT/MCSE/MCITP/MCTS/MCSA/CCSE/CCSA/CCNA/A+®
E-mail: sergey@infosec.co.il
Mob: (+972) 526848757

4.6. Designing Auditing

To design an audit policy, complete the following steps:

1. Identify the objects that require auditing and the potential security threats.
2. Enable the audit policy that records events related to the objects, events, and threats you've identified. Indicate whether to track success or failure (or both).
3. If necessary, configure auditing for specific files and objects. You must configure auditing on specific objects to audit the following:
    - NTFS file or folder access
    - Printer access
    - Active Directory object access
    - Certificate Authority actions
    - Registry hive, key, or subkey access
    - IIS metabase object access

Although you might be tempted to audit everything, you should audit only those events that are necessary to ensure a secure network. Use the following guidelines when designing auditing.

- Audit only what's necessary.
    - Audit for Success only or Failure only if either one if sufficient to give you the information you need.
    - Enable auditing on only the necessary objects. For example, enable auditing on specific files or registry keys rather than enabling auditing on an entire drive or registry hive.

    Excessive auditing uses processor cycles and requires disk space for the audit log. In addition, auditing every event increases the number of entries in the log, making it harder to find those things you are looking for.

- Make sure you have modified the audit log size and characteristics so that you are saving the data you want to save where you want it.
- Archive audit logs so you can review past data if you suspect a problem.

- Identify actions that should always be audited. In addition, periodically audit other actions for short periods of time to catch any unforeseen problems.
- Design periodic reviews of audit logs. Auditing is useless if you do not read the logs.
- For investigative and evidentiary reasons, make sure that all pertinent events are getting recorded to the Security log. In addition to tracking the necessary events, make sure your logs are properly configured to save all of the necessary information.
    - Use the Event Log policies in Group Policy to configure the Security log size and retention method.
    - To preserve all logged actions, configure logs to *not* overwrite events. When logs are not configured to clear automatically, you must periodically save and clear the logs to make room for additional events.
    - Enable the **Audit: Shut down system immediately if unable to log security audits** security option to prevent the system from being used if the log is full (this setting is also referred to as **CrashOnAuditFail**).

© Sergey Gorokhod
MCT/MCSE/MCITP/MCTS/MCSA/CCSE/CCSA/CCNA/A+®
E-mail: sergey@infosec.co.il
Mob: (+972) 526848757