Whitepaper

Interaction with Active Directory

DriveLock use AD

DriveLock SE 2017

Contents

1 Introduction

DriveLock is the perfect solution to prevent unauthorized data transfer by protecting and locking all sorts of device types and interfaces connected to a computer. Access to particular devices can be granted to certain users and groups providing familiar handling of data.

The ability to configure DriveLock settings using Active Directory group policy allows for a centralized and easy configuration of an entire enterprise network.

This document provides technical information to display interaction between DriveLock and Microsoft Active Directory.

Careful planning and evaluation is an essential preliminary step for successfully deploying DriveLock throughout the enterprise. This paper also discusses best practices and examples of how to meet the specific needs of your organization.

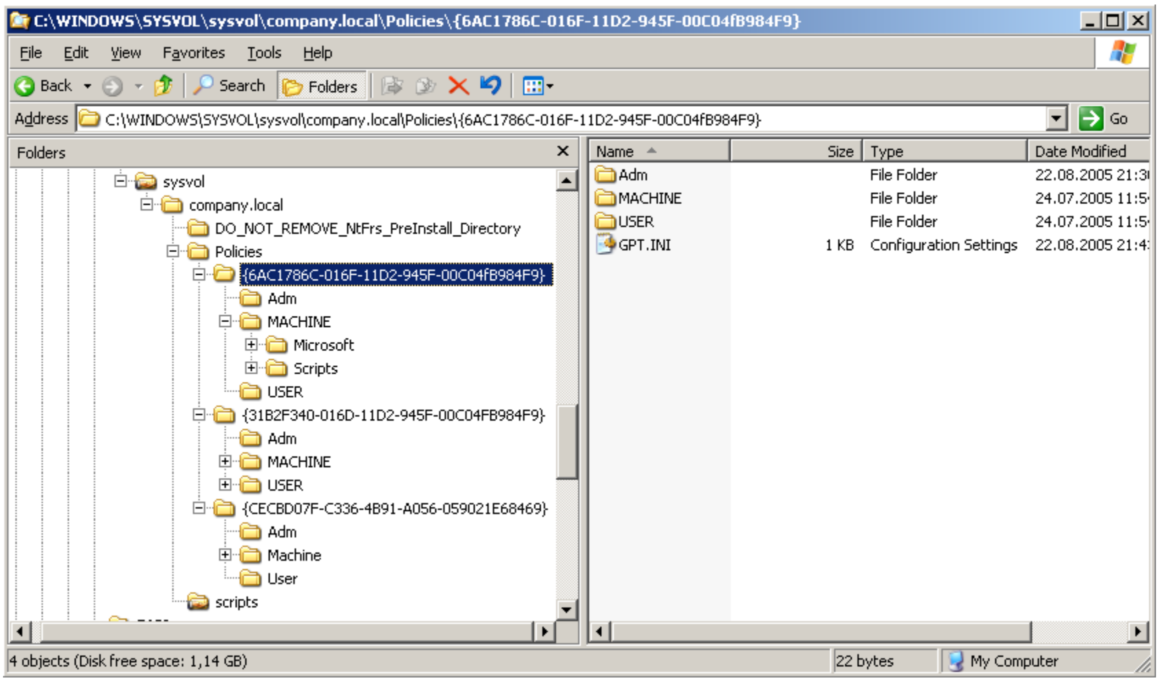
2 Group policy

Group policy provides a powerful method for managing many aspects of an enterprise environment based on Active Directory. It scales up to the largest deployments, is fast to deploy, but can also accommodate specific needs of small groups – all at the same time.

Group policy settings are stored in Active Directory (i.e. on Domain Controllers) and are replicated within a domain. To be more precise, group policy objects are stored in two places:

- Configuration data in Active Directory
- Template data in form of files and directories in the system volume (Sysvol)

Therefore, each group policy object consists of an object holding configuration data that is linked to a directory holding template data.



C:\WINDOWS\SYSVOL\sysvol\company.local\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}

```
sysvol
  company.local
    DO_NOT_REMOVE_NtFrs_PreInstall_Directory
    Policies
      {6AC1786C-016F-11D2-945F-00C04fB984F9}
        Adm
        MACHINE
          Microsoft
          Scripts
        USER
      {31B2F340-016D-11D2-945F-00C04FB984F9}
        Adm
        MACHINE
        USER
      {CECBD07F-C336-4B91-A056-059021E68469}
        Adm
        Machine
        User
    scripts
```

Name	Size	Type	Date Modified
Adm		File Folder	22.08.2005 21:3
MACHINE		File Folder	24.07.2005 11:5
USER		File Folder	24.07.2005 11:5
GPT.INI	1 KB	Configuration Settings	22.08.2005 21:4

4 objects (Disk free space: 1,14 GB) 22 bytes My Computer

Figure 1: Sysvol structure on a domain controller

DriveLock stores configuration settings in the template data area (in the registry.pol to be precise, located in the MACHINE-Folder of the corresponding group policy object).

Each group policy object has a publishing point, also known as the link information, indicating the site, domain, or organizational unit to which a group policy is applied. Security filtering enables an administrator to target sets of specific objects (users, groups, computers ...). Group Policy objects include two sections (computer and user settings) that can each be disabled.

3 Organizational units

DriveLock uses group policy to deploy appropriate settings to computers that are members of an Active Directory domain, so user settings are not used. Settings are applied by the DriveLock agent running on these computers.

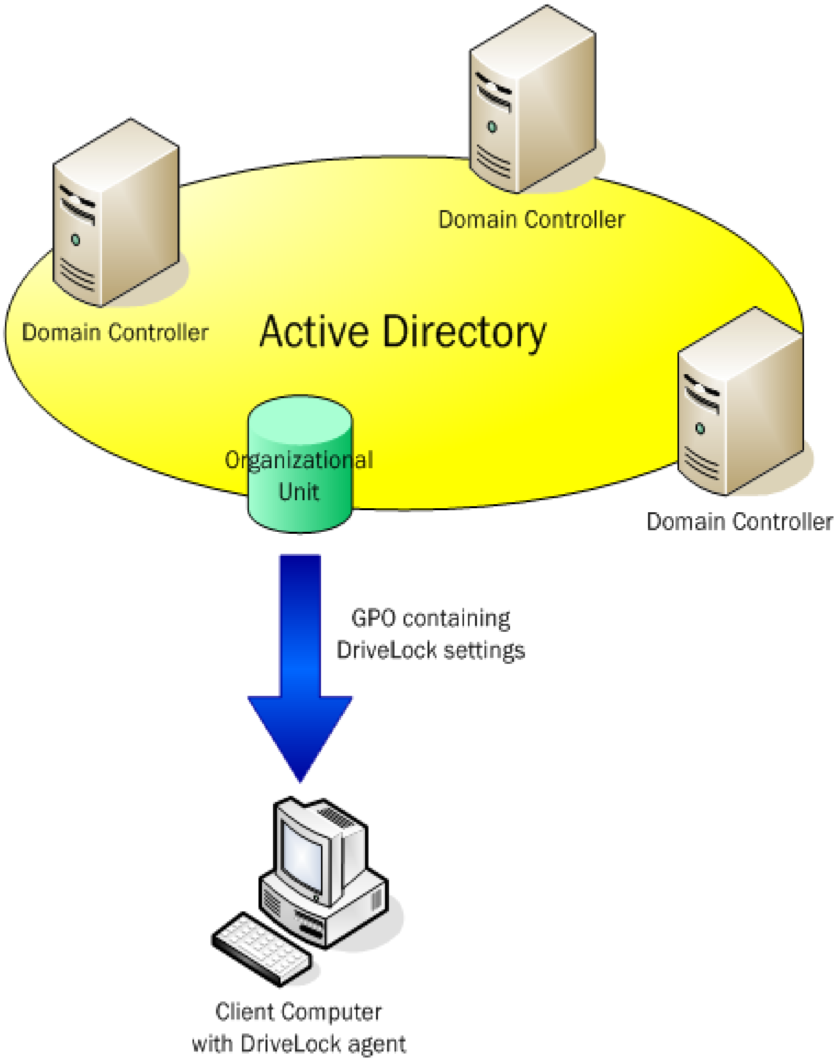


Figure 2: Ring topology replication used by FRS

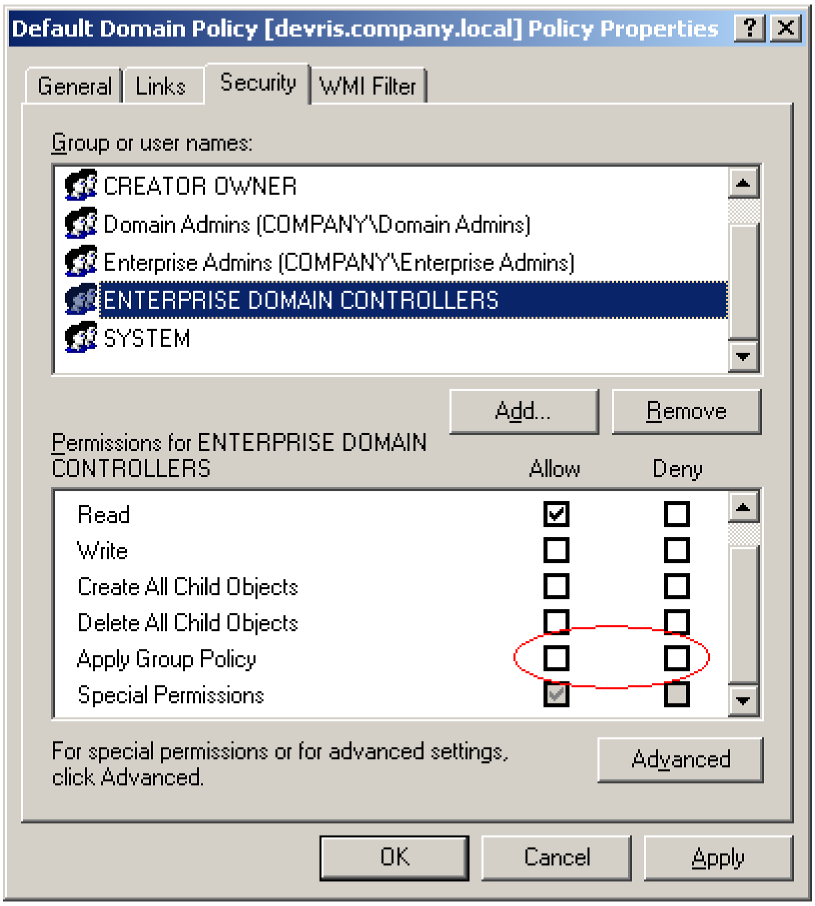
As computers are often arranged in organizational units to display a certain affiliation to a department or business unit, it is common practice to link group policy objects containing DriveLock settings to organizational units.

Another key factor in favor of that practice is delegation of administrative rights. Furthermore, using group policy objects on domain or site level makes it difficult to maintain graded protection levels along departmental unit structures.

Hence, it is recommended to deploy DriveLock settings using group policy at the organizational unit level.

4 Selective adaptation of DriveLock settings

In case different DriveLock settings cannot be categorized on boundaries of several organizational units, distinctive settings within an organizational unit can be realized by configuring the security properties of the corresponding group policy object.



Group or user names:

- CREATOR OWNER
- Domain Admins (COMPANY\Domain Admins)
- Enterprise Admins (COMPANY\Enterprise Admins)
- ENTERPRISE DOMAIN CONTROLLERS
- SYSTEM

Permissions for ENTERPRISE DOMAIN CONTROLLERS	Allow	Deny
Read	☑	□
Write	□	□
Create All Child Objects	□	□
Delete All Child Objects	□	□
Apply Group Policy	□	□
Special Permissions	☑	□

For special permissions or for advanced settings, click Advanced.

Figure 3: Security settings on a group policy object

By activating “Apply Group Policy” for specified groups of computers, the application of group policy settings can be controlled to meet required needs.

Several group policy objects containing different DriveLock settings and linked to the same organizational unit are manageable by using this technique regardless of the overall organizational unit structure.

5 Replication of Active Directory

As already mentioned, DriveLock stores its configuration – using group policy – in the system volume (Sysvol) which is replicated within the domain by the file replication service (FRS).

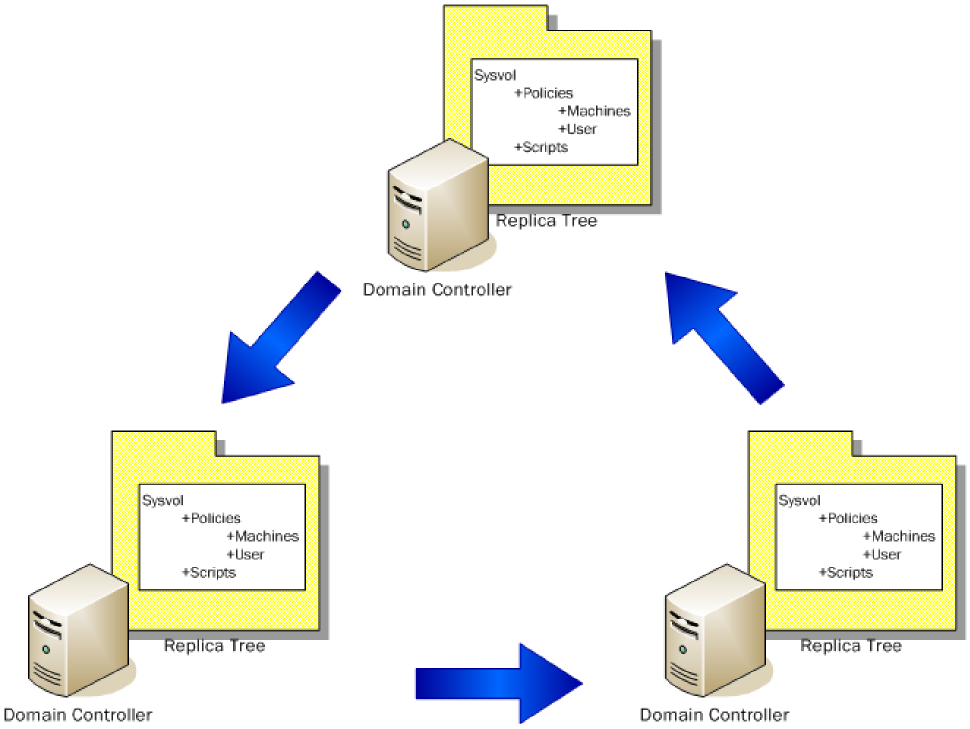


Figure 4: Ring topology replication used by FRS

This built-in replication functionality provides consistent and up-to-date group policy objects on every domain controller. Domain member computers apply the specified settings during startup and defined refresh cycles using their client side extensions. This mechanism takes care that DriveLock settings are distributed to client computers.

A working FRS is crucial to Active Directory and group policy operation. If FRS is not replicating properly, users can experience a variety of hard to identify problems related to settings applied by group policy. Therefore, the health of FRS is essential to proper DriveLock operation and should be monitored on a regular basis. Microsoft provides a monitoring tool called Ultrasound to troubleshoot replication issues.

Problems regarding not applied or incorrect DriveLock settings often find their cause in damaged group policy objects aroused by improper replication.

6 Replication traffic

Group policy objects are replicated to every domain controller in an Active Directory domain. Client computers fetch the group policy settings from the domain controller located in the same site. A site in Active directory is a region of your network with high bandwidth connectivity and by definition a collection of well-connected computers, based on TCP/IP-Subnets.

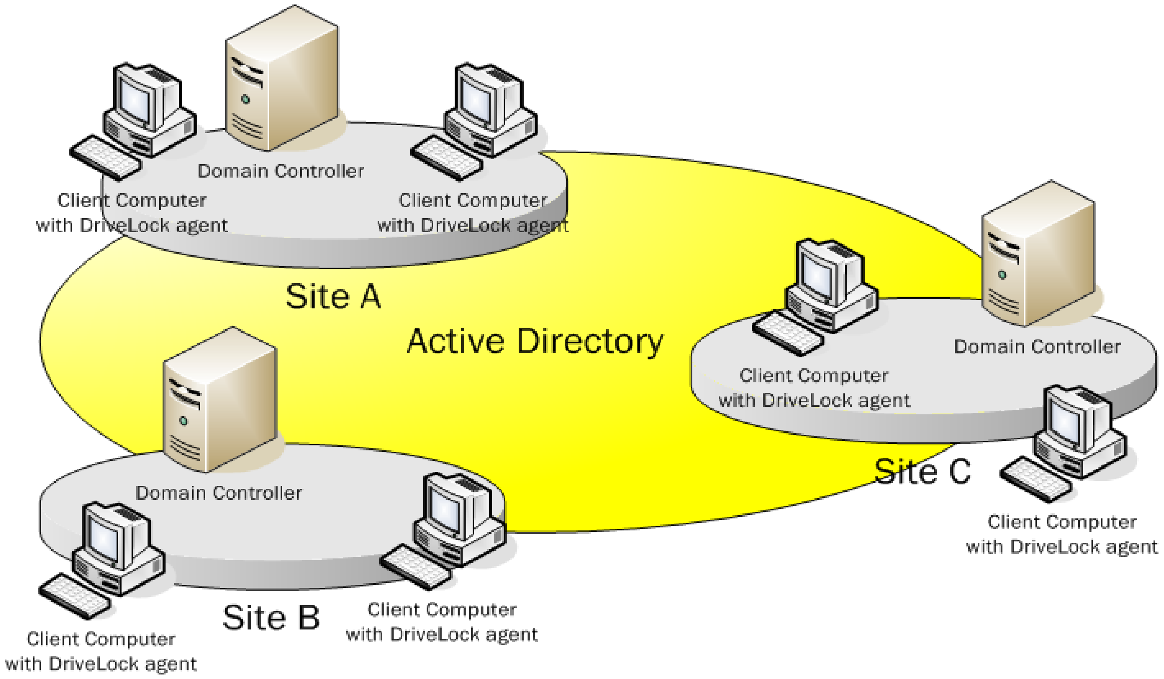

Domain Controller
Client Computer with DriveLock agent
Client Computer with DriveLock agent
Site A
Active Directory
Domain Controller
Client Computer with DriveLock agent
Site C
Client Computer with DriveLock agent
Domain Controller
Site B
Client Computer with DriveLock agent
Client Computer with DriveLock agent

Figure 5: Active Directory with defined sites

The concept of sites enables client computers to determine their position on the network, contact the nearest domain controller, and obtain needed information without arousing network traffic over WAN links.

As DriveLock depends on group policy objects to deploy its settings to client computers, the obvious question to make reliable predictions about replication traffic is:

How much space does a group policy object containing DriveLock settings use?

This depends on the defined settings and the number of group policy objects.

To get a more precise answer, let us have a look at the following spreadsheet (Figure 6):

Settings		Used space (KB)
General	General settings (Includes all general settings like event handing, encryption etc.)	0.5
Drives	Default settings (Includes general settings such as locking of drive types USB, Firewire, CD/DVD etc.)	1.1
	Exceptions (Whitelist rules)	0.4 (per exception)
Devices	Default settings (Includes general settings such as state of device classes)	2.7
	Templates	22.1 (per template)
	Whitelist rules (no template-generated rules)	0.4 (per rule)
Network profiles	Default settings (Includes general settings such as notification and WiFi locking)	0,2
	Locations (Includes properties of a location)	3,5 (per rule)
	Configuration profile (Includes properties to set for each location)	5,2 (per rule)
Applications	Default settings (Includes general settings such as ALF operating mode)	0,2
	Templates (Depends on the amount of applications per template. Example Office 2007)	60 (per template)
	Rules (Includes single application)	3,2 (per rule)
	Hash database (Includes all applications of a computer.	180 (per database)
Encryption	Default settings (Includes encryption algorithm, file system, and so on)	3
	Container password / certificate (Includes password and certificate for recovery)	5
	Enforce encryption (Includes settings for automatic encryption)	2
	Full Disk Encryption (FDE) (Includes all settings and certificates for FDE)	8

As can be derived from the above figure, required space of a group policy object used for DriveLock settings heavily depends on the number and sort of settings configured.

A standard DriveLock group policy object needs approximately 5 KB (no templates defined).

Once the DriveLock group policy object is replicated throughout the Active Directory domain, new replications do not occur before settings are changed or added. In addition, client computers cache group policy objects locally until they change.

DriveLock settings are more or less static (usually, they are not changed every day); therefore, after initial Active Directory replication and adoption by client computers replication traffic only occurs when settings change.

7 Exchange DriveLock settings between domains

Active Directory enterprise environments often comprise more than one domain with DriveLock in use. Additionally, DriveLock group policy objects throughout domains frequently consist of nearly identical settings. To make life easier, the DriveLock Configuration Management Tool (dlpolmig.exe) allows for simplified export and import of DriveLock settings.

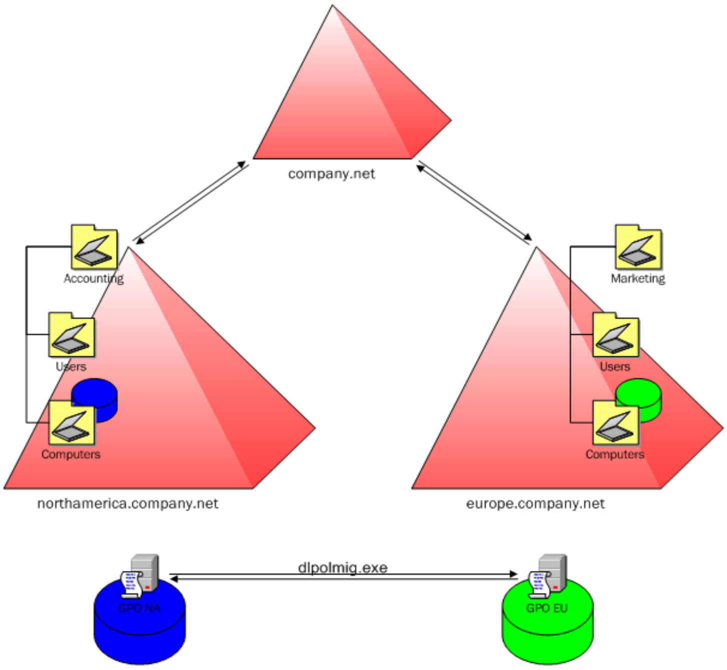


Figure 6: Typical DriveLock operation environment with two domains

This tool can also be used in conjunction with common scripting techniques to automate distribution of DriveLock configuration settings and to enforce consistent protection levels throughout domain boundaries. Please consult Appendix A for further information and specific command-line switches.

8 Real-world implementation

Now that we have discussed the decisive factors about interaction between DriveLock and Active Directory, let us face the real world. The following example shows a classical DriveLock deployment in an enterprise environment of 48,000 client computers.

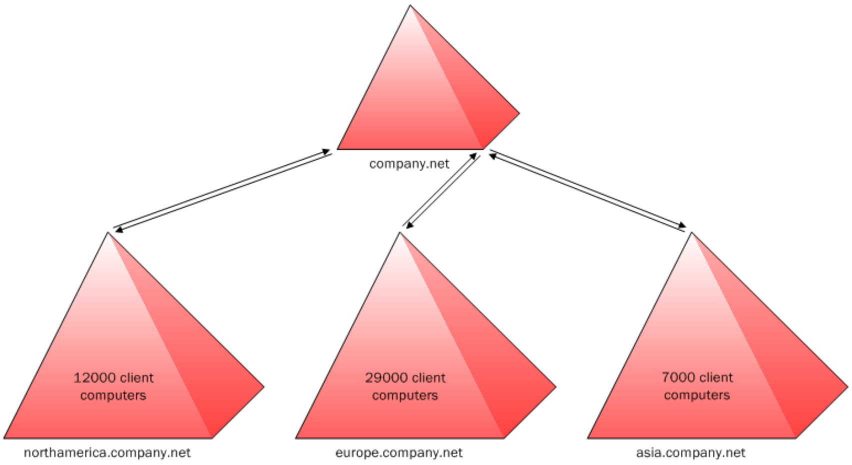


Figure 7: Overview of the Active Directory real-world example (domain structure)

The domain structure is based on the worldwide locations where the company is represented. A top-level domain is used exclusively for administrative purposes.

The basic structure of the organizational units is nearly identical in the three domains containing client computers. As we can see, the largest and most challenging domain in respect of administration and replication is the European one (Figure 9).

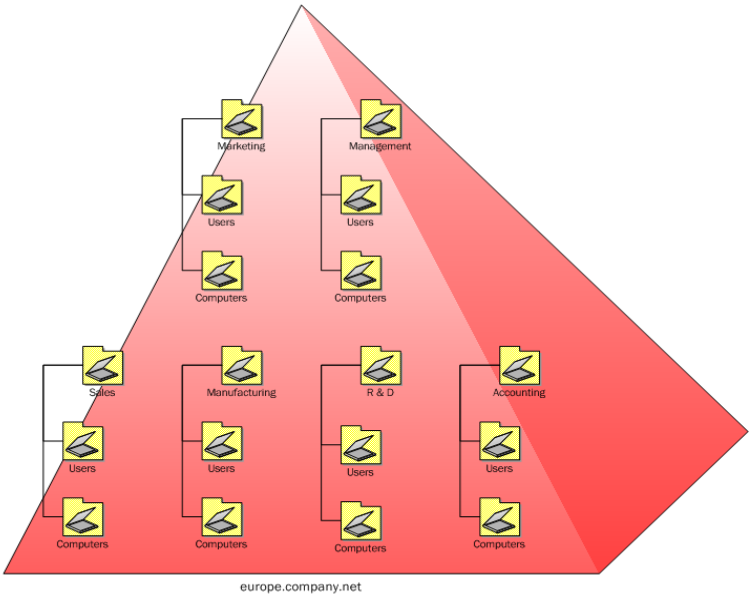
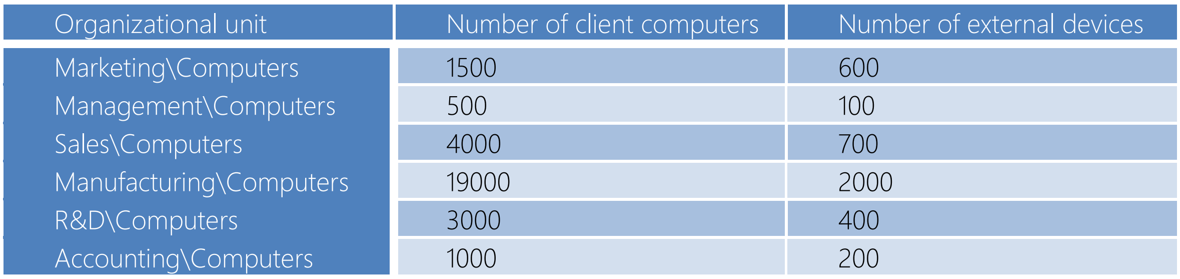


Figure 8: Organizational unit structure (based on the European domain)

The 29,000 client computers of the European domain are distributed among the organizational units as follows:



Organizational unit	Number of client computers	Number of external devices
Marketing\Computers	1500	600
Management\Computers	500	100
Sales\Computers	4000	700
Manufacturing\Computers	19000	2000
R&D\Computers	3000	400
Accounting\Computers	1000	200

Figure 9: Spreadsheet (organizational units, no. of client computers, and no. of external devices)

Based on the number of client computers and the respective usage pattern of external devices in the various organizational units the following implementation of group policy objects containing DriveLock settings is recommended:

- Many external devices are used within the Manufacturing unit. Once attached, they normally do not change. Therefore, we use a dedicated DriveLock group policy object despite the large number of client computers and devices.
- For security reasons client computers in the R&D, Management and Accounting units must have tightly locked down settings regarding external devices. This can be taken into account by using a separate DriveLock group policy object for these three units.
- Quite a few external devices are used in the Marketing and Sales units; additionally, devices are often upgraded or replaced by new ones. We use another group policy object to restrict replication traffic despite of the many setting changes that take place.

Therefore, we end up with implementing three different DriveLock group policy objects linked to the respective organizational units:

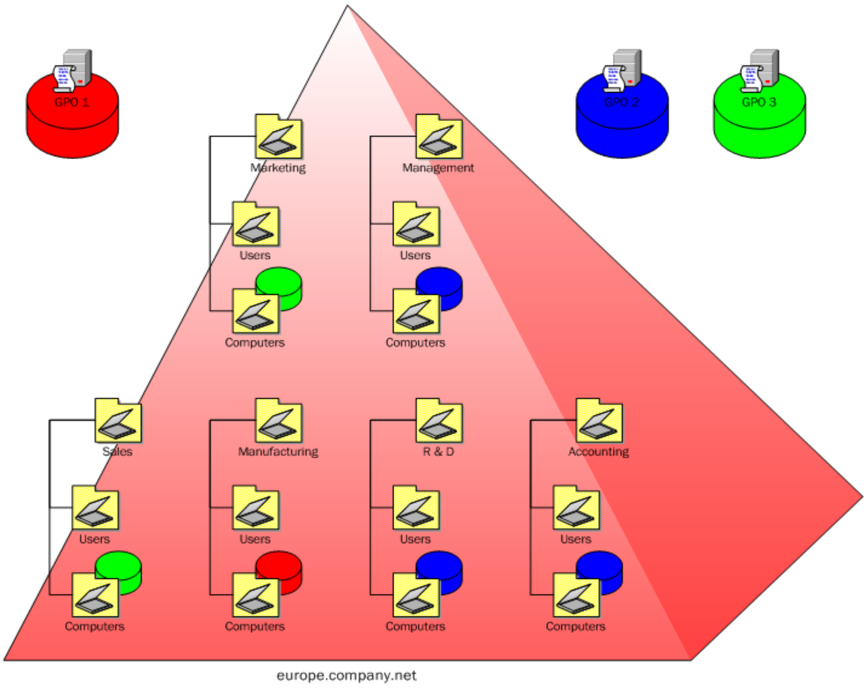


Figure 10: Organizational unit structure with linked DriveLock group policy objects

9 Best practices

Now that we have seen the underlying Active Directory techniques, know about the interaction of DriveLock with these, and looked at an example scenario the following list summarizes the most important Do's and Don'ts.

- When creating a group policy object allotted to DriveLock configuration, only configure settings that are related to DriveLock. This simplifies administration and allows for easier troubleshooting.
- Disable the user configuration settings portion of the DriveLock group policy object, as DriveLock settings apply only to computer objects.
- To optimize replication traffic, consider using a separate group policy object for client computers with often changing devices and users.
- Computers having relatively fixed assigned users and devices can be managed in large numbers by a single DriveLock group policy object.
- Avoid linking DriveLock group policy objects to the domain or site level.

Have in mind that the above rules are meant for larger enterprise environments containing 10.000 or more client computers to be managed by DriveLock. As users normally do not change their external devices very often, DriveLock settings are more or less static and do not require frequent group policy updates.

Additionally, companies with only hundreds or a few thousand client computers and scarcely changing removable devices do not have to pay much attention to replication issues.

10 Appendix A

-*command-line switches for the Configuration Management Tool (dlpolmig.exe)*

Introduction

The DriveLock Configuration Management Tool (dlpolmig) can be used to export, import or copy DriveLock configuration settings from and to various sources.

```
C:\Program Files\CenterTools\DriveLock MMC\Tools>dlpolmig -?
```

Usage:

```
DLPolMig    -src {file | cfgfile | gpo | local}

            -srcpath {<file> | <gpo> | browse}

            -tgt {file | cfgfile | gpo | local}

            -tgtpath {<file> | <gpo> | browse}

            [-newgpo <gpo friendly name>]

            [-sidtrans]

            [-inc]

            [-mapdom <sourcedom> <targetdom>]

            [-mapprefix <sourceprefix> <targetprefix>]

            [-mapsuffix <sourcesuffix> <targetsuffix>]
```

Import, export, or copy DriveLock configuration settings from and to various sources.

Parameters:

-src Data source, can be

file ... read from DLC file

cfgfile ... read from configuration file

gpo ... read from Group Policy Object

gpo5 ... read from Group Policy Object in DriveLock 5 format

local ... read from local computer (local configuration)

-srcpath Path to the source location, specify

- full path and file name (DLR) for source type "file"

- Group Policy Object path for source type "gpo"

- "browse" to browse for the object

-tgt Target type, can be...

file ... write to DLC file

cfgfile ... write to configuration file

gpo ... write to Group Policy Object

gpo5 ... write to Group Policy Object in DriveLock 5 format

local ... write to local computer (local configuration)

-tgtpath Path to the target location, specify

- full path and file name for target type "file"

- Group Policy Object path for target type "gpo"

- Domain path if "-newgpo" is specified and target type "gpo"

- "browse" to browse for the object

-newgpo Create a new Group Policy Object instead of using an existing one

as the target. Specify the GPO's friendly name after "-newgpo"

-sidtrans Translate SIDs. This resolves all SIDs to domain / account namesand maps names as defined. When exporting to a file this store additional information (name, domain) in the file.

-inc Add source settings to target. Only works for targets GPO5, local

-mapdom Maps account domain names. Only works with -sidtrans specified. Specify source domain (NetBIOS name) as first parameter, target domain (NetBIOS name) as second. Replaces all occurrences of source with target domain. Switch may specified more than once.

-mapprefix Maps account name prefixes. Only works with -sidtrans specified. Specify source prefix as first parameter, target prefix as second parameter. Replaces specified source prefix with target prefix in all user/group names. Switch may specified more than once.

-mapsuffix Maps account name suffixes. Only works with -sidtrans specified. Specify source suffix as first parameter, target suffix as second parameter. Replaces specified source suffix with target suffix in all user/group names. Switch may specified more than once.

-h -? Show help screen

Notes:

The tool can copy from any to any source.

SID translation will not work when copying from file to file.

Specify a GPO object path in the form:

```
LDAP://CN={<guid>},CN=Policies,CN=System,DC=...
```

An existing target file will be overwritten without warning.

A target GPO must exist and will not be created unless -newgpo is specified.

Samples: Export GPO to file:

```
DLPolMig -src gpo -srcpath browse -tgt file -tgtpath c:\mypol.dlr
```

Export GPO to file with SID translation (store account names in file):

```
DLPolMig -src gpo -srcpath browse -tgt gpo -tgtpath browse -sidtrans
```

Import GPO from file with SID translation, replace domain LONDON by MUNICH, replace in all accounts prefix "UK-LON-" with "DE-MUC-":

DLPolMig -src file -srcpath browse -tgt gpo -tgtpath browse -sidtrans -mapdom LONDON MUNICH -mapprefix UK-LON- DE-MUC-

Copyright