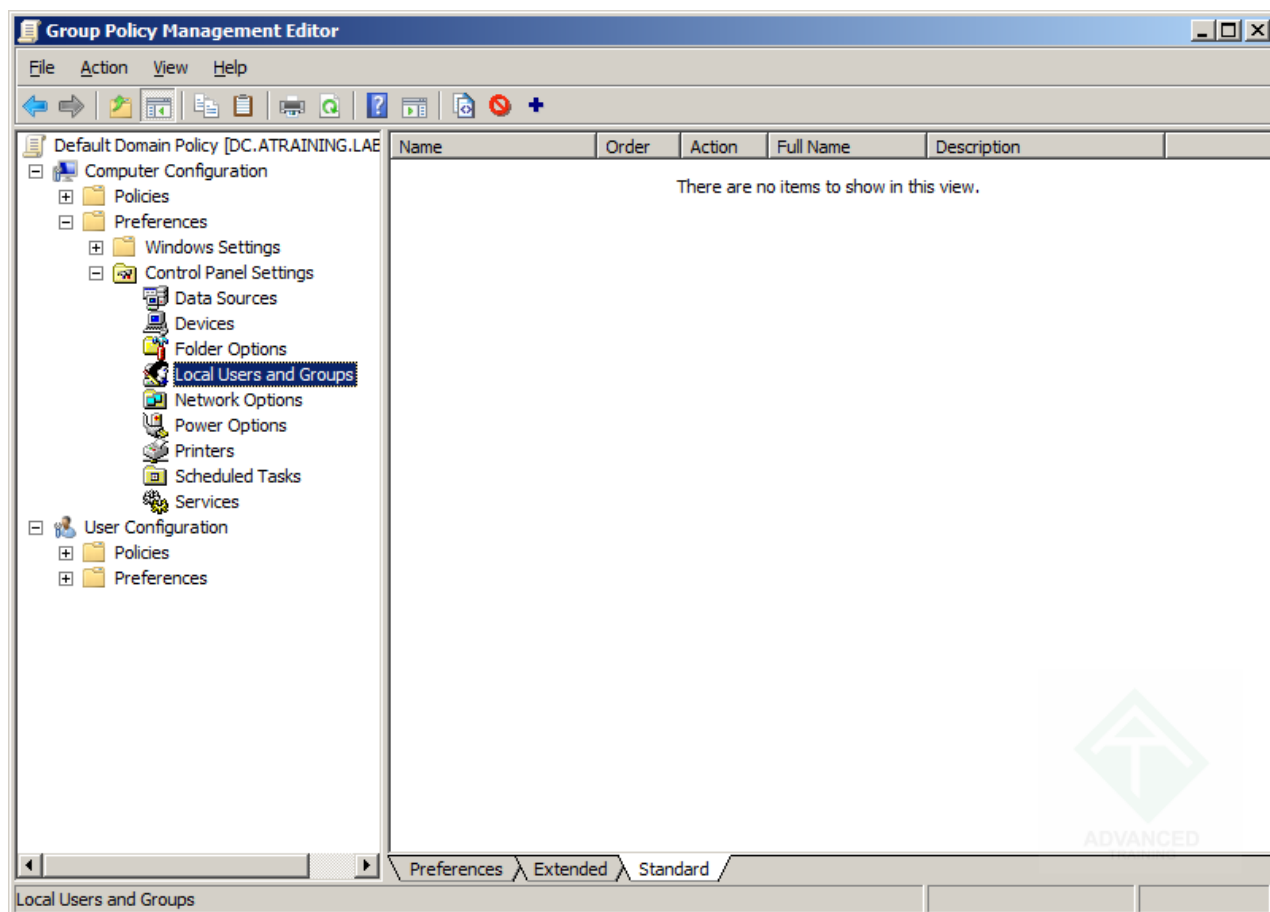


Управление локальными паролями администраторов на доменных машинах - достаточно древняя и до сих пор актуальная задача. LAPS помогает сделать всё просто, удобно и красиво.

 atrainig.ru/laps-local-administrator-password-solution

2015-05-04T02:51:24+08:00



Привет.

Управление локальными паролями администраторов на доменных машинах – достаточно древняя и до сих пор актуальная задача.

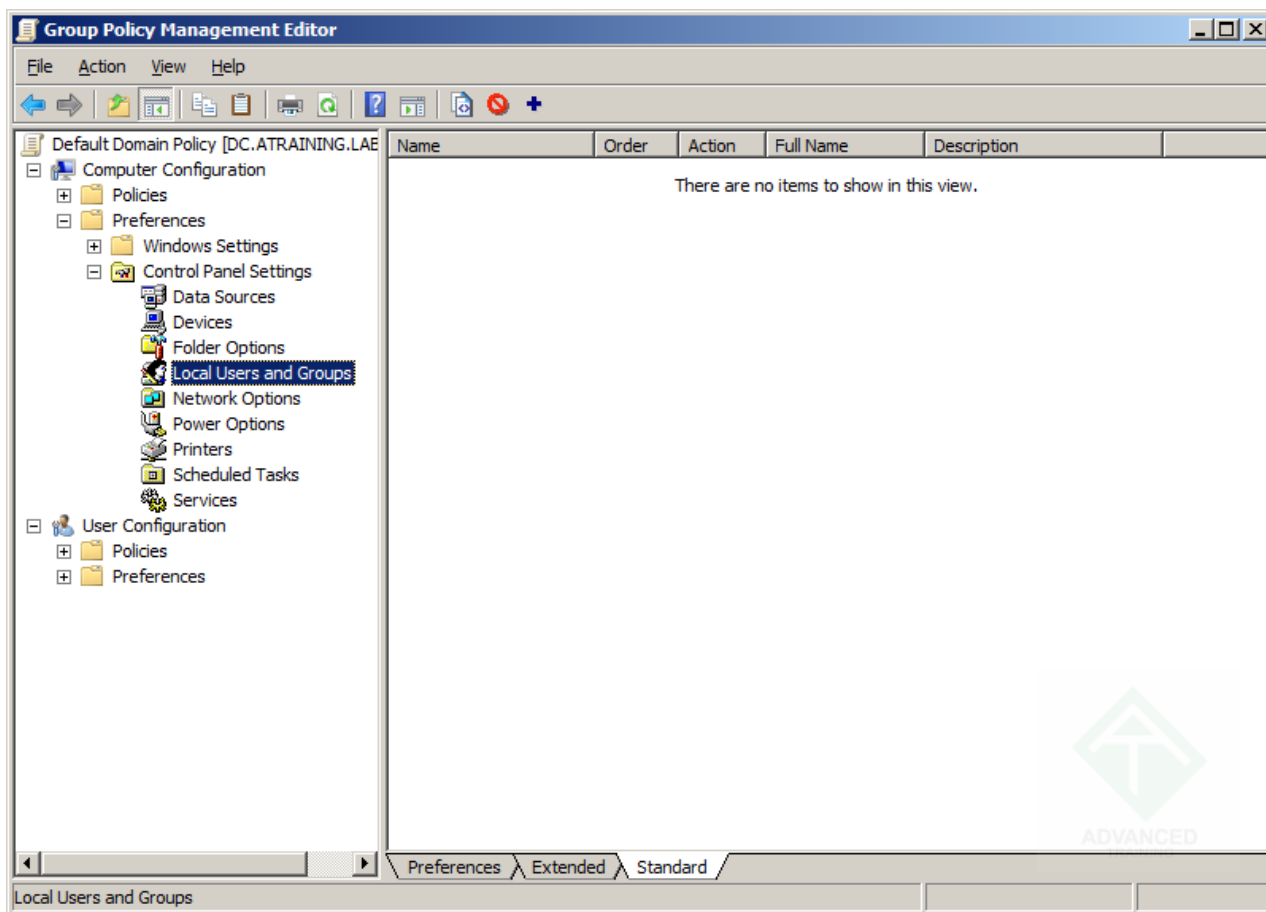
Ведь по сути, жизненный цикл учётной записи администратора, в плане продолжительности, равен жизненному циклу рабочей станции – поэтому задачи защиты этой учётной записи от НСД, периодической смены пароля на известный IT-отделу (чтобы можно было проводить в случае форс-мажора какие-либо нужные действия), отслеживание нецелевого использования (как локального, так и удалённого – ведь знающий этот пароль в обычной ситуации может удалённо подключаться к системе и проводить различные действия) – все эти и множество других, более мелких, но нужных задач – они отнимают много времени и снижают общий уровень безопасности домена.

Обычно используются различные ухищрения и их комбинации, чтобы упростить эту ситуацию. Например:

- Централизованно переименовать учётную запись локального администратора на рабочих станциях
- Отключить её (хотя всё равно при входе в Safe Mode она автоматически включается)
- Поставить на logon script что-то сигнализирующее о входе локальным администратором и ввести за это кары
- Придумать огромный и сложный пароль (вариант – написать скрипт, который обходит workstations и member servers в Active Directory и меняет там, используя специальную техническую доменную учётку, пароль локальной учётной записи администратора, отписывая в отдельный файл новый пароль или, в случае неудачи операции, код ошибки)
- Варварский метод, который я в своё время очень любил – физически удалить учётную запись локального администратора из SAM и переименовать гостя в админа – тогда взломавший эту учётную запись пользователь будет долго медитировать над странными околонулевыми правами на системе

Все эти варианты чем-то снижают проблематику, но не убирают её. Организовывать сложную систему постоянного мониторинга за статусом этой учётной записи, не отредактировали ли её, не зашли ли ей, не запустили ли что-то от неё – трудоёмко и опять-таки не спасает от всех ситуаций НСД – например от того, что продвинутый пользователь скачает утилиту, которая позволит на загрузке сбросить пароль локального админа. Но задачи управления этой учётной записью и безопасного и автоматического обновления её пароля всё ж решаемы.

Начиная с NT 6.0 у вас появились Group Policy Preferences, которые тоже могут помочь в этом деле:



[Управление локальными учётными записями через Group Policy Preferences \(кликните для увеличения до 801 px на 572 px\)](#)

New Local User Properties

Local User | Common

Action: Update

User name: Administrator (built-in)

Rename to: Administrator (built-in)
Guest (built-in)

Full name:

Description:

Password:

Confirm Password:

☐ User must change password at next logon

☐ User cannot change password

☐ Password never expires

☐ Account is disabled

☒ Account never expires

Account expires: 7/19/2015

OK Cancel Apply Help

[Изменение пароля локального администратора через Group Policy Preferences \(кликните для увеличения до 404 px на 448 px\)](#)

Но неприятность в том, что данный пароль будет лежать в легковосстановимом виде в папке SYSVOL, вместе с остальными данными GPP. Так что проблемы остаются.

Эти вопросы – и некоторые другие – можно решать более цивилизованным способом – используя [LAPS](#).

Давайте разберёмся. Я предполагаю, что вы знаете вопросы работы Active Directory хотя бы на уровне простенького бесплатного курса [Microsoft 20410D](#), поэтому в отдельные совсем уж тривиальные детали углубляться не буду.

Использование LAPS (Local Administrator Password Solution)

- Что умеет LAPS
- Разворачиваем LAPS по шагам
- Ставим LAPS на рабочее место администратора
- Расширяем схему для LAPS
- Подготовка домена для LAPS GPO
- Подготовка для работы с LAPS RODC
- Защищаем хранение паролей в Active Directory
- Настраиваем политики LAPS для рабочих станций и member-серверов
- Развёртываем LAPS для клиентов – рабочих станций и member-серверов

Начнём.

Что умеет LAPS

Local Administrator Password Solution представляет из себя сочетание:

- Локально устанавливаемого на управляемых рабочих станциях (и серверах, замечу) ПО, которое, по сути, добавляет ещё один компонент к Group Policy Client Side Extension;
- Расширения схемы Active Directory (два новых атрибута для класса computer, нужные для хранения паролей локальных администраторов и некоторых доп.атрибутов);
- Дополнительных административных шаблонов для групповых политик;
- Модуля PowerShell для автоматизации всех задач управления LAPS;
- Утилиту для управления через GUI;

Всё это позволяет:

- Безопасно хранить в Active Directory пароль локального администратора для каждой рабочей станции (а также member server'ов)
- Устанавливать правила для пароля (длину, критерий сложности)
- Менять пароль локального администратора через Active Directory, без необходимости прямого подключения к целевой системе – при этом делать это безопасно, в рамках применения групповых политик, по защищённому каналу
- Устанавливать срок истечения времени действия пароля локального администратора и автоматически менять его (безусловно, и на локальной машине, и в Active Directory)

Работать всё это будет на инфраструктуре, построенной на DC уровня Windows Server 2003 и выше, и управлять паролями на системах, построенных на базе серверной ОС Windows Server 2003 и клиентской ОС Windows Vista. Да, XP официально не поддерживается, увы – но можно использовать приведённый выше пример с Group Policy Preferences, ведь на Windows XP SP3 модуль обработки GPP ставится как обновление.

Разворачиваем LAPS

Я буду разворачивать актуальный на июль 2015го года LAPS 6.1. Для приближенности к боевой ситуации это будет сделано на Windows Server 2008 R2 (что, впрочем, ничего не меняет в функционале LAPS) – разве что, для того, чтобы корректно отработали powershell-скрипты мне нужно будет обновить Windows Management Framework – я поставлю версию 4.0 вот отсюда:

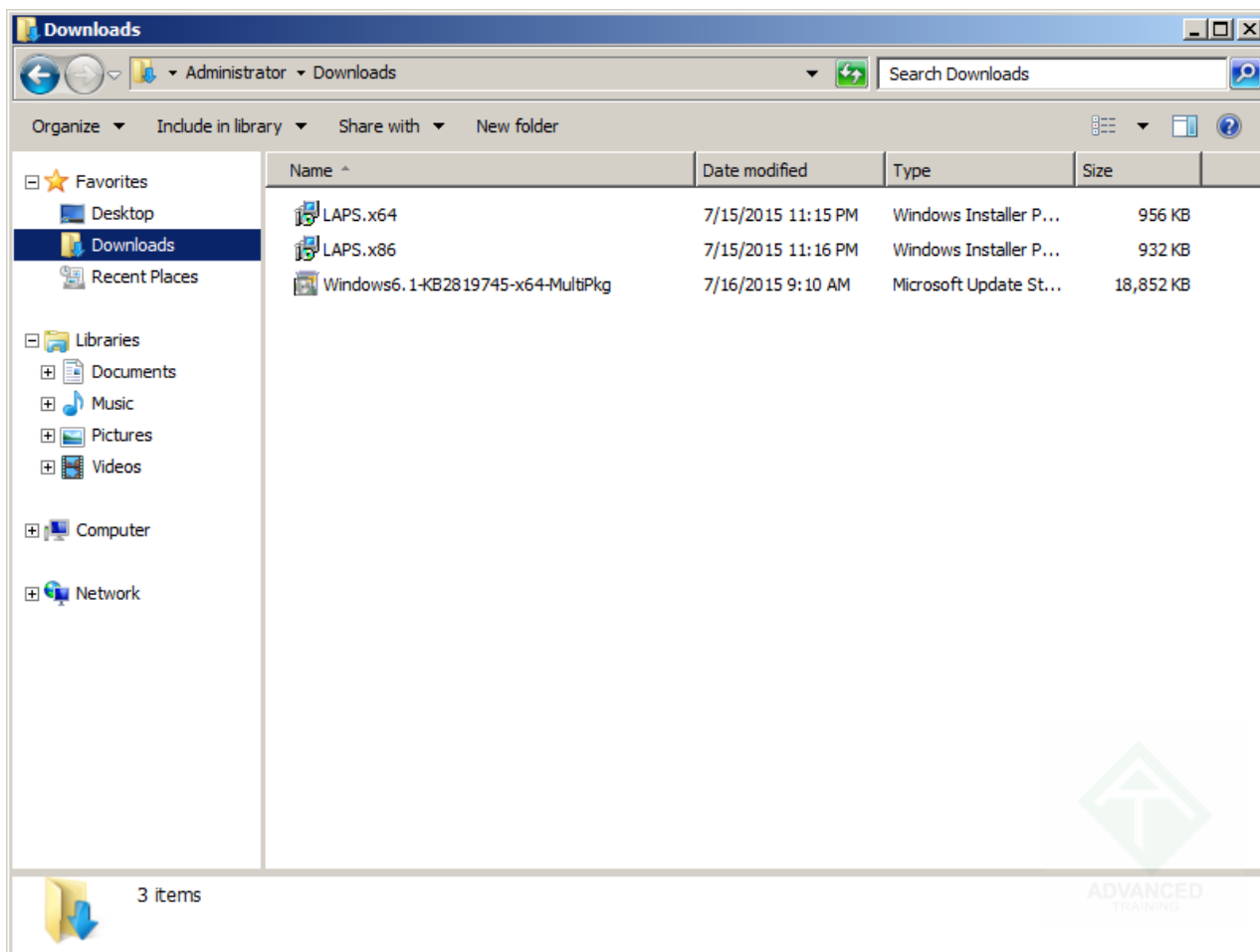
<http://www.microsoft.com/en-us/download/confirmation.aspx?id=40855>.

Этот шаг не нужен, если Вы будете ставить Local Administrator Password Solution на, допустим, Windows Server 2012 R2 – но в большинстве инфраструктур на DC всё же используются не самые топовые ОС, поэтому данный шаг потребуется. LAPS же, повторюсь, будет работать одинаково и на Windows Server 2008 R2, и на Windows Server 2003.

Загружаем нужное

LAPS версии 6.1: [отсюда](#). Из компонентов нам понадобятся оба дистрибутива LAPS – что для x86, что для x64 систем – они равнозначны, но, скорее всего, понадобятся оба – исключение составит лишь инфраструктура, где или только 32х битовые системы, или только 64х битовые – а это случай довольно-таки редкий.

WMF версии 4.0 (я ставлю именно её как самую последнюю из RTM-версий на момент написания статьи – а так, грамотный администратор в принципе должен заранее упростить себе работу, обновляя WMF на серверах со старыми версиями ОС): [отсюда](#). В результате у нас будет что-то такое:

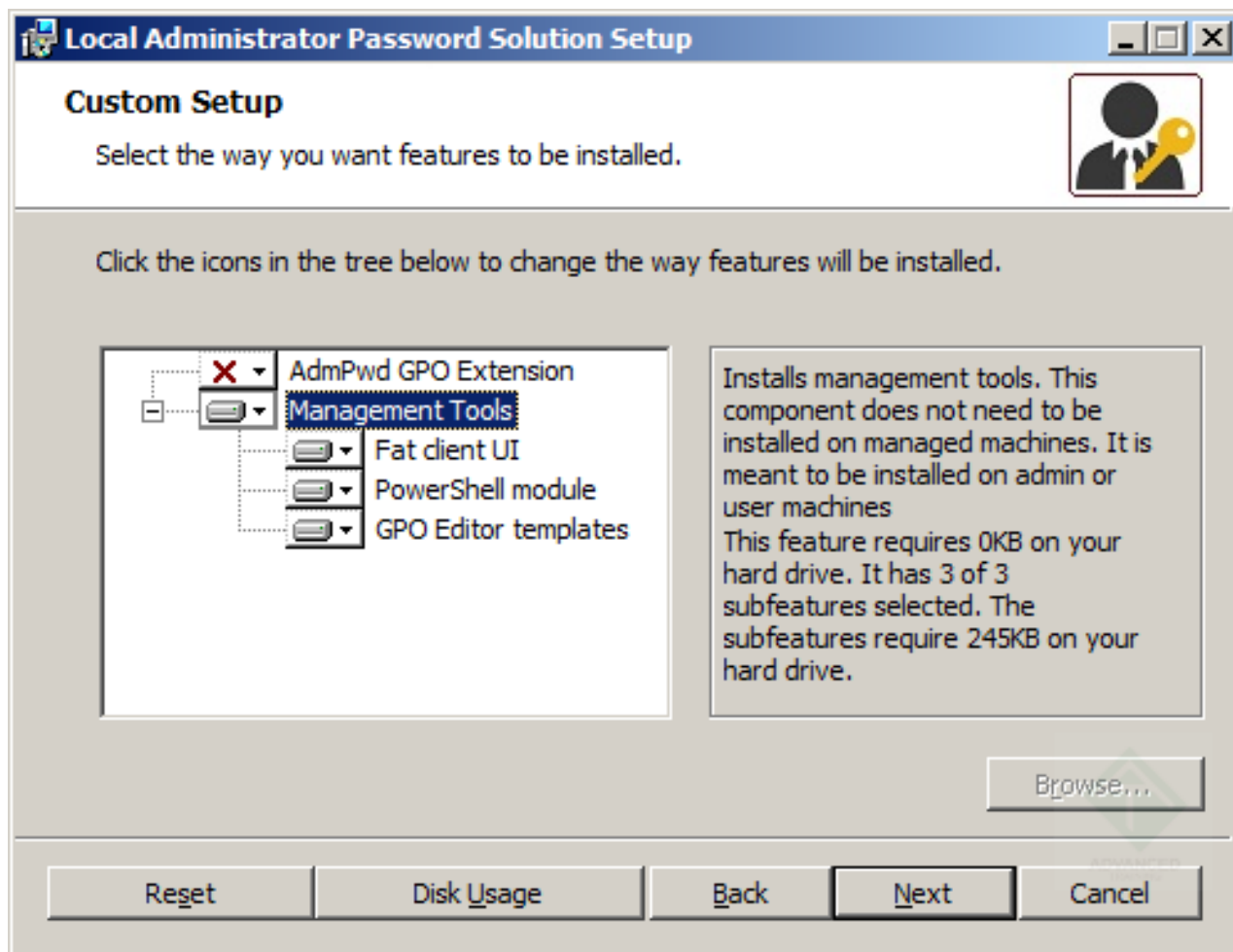


[Загрузка LAPS \(Local Administrator Password Solution\)](#)
(кликните для увеличения до 800 px на 600 px)

ОК, теперь начнём установку.

Ставим LAPS на рабочее место администратора

Первым делом нам надо установить полновесный комплект LAPS на рабочее место администратора. Часть операций (например, расширение схемы и выгрузка в общее хранилище политик) будет делаться разово и больше не потребуется – ну а, допустим, установка “толстого” GUI-клиента может проводиться там, где удобно. Так как я ставлю LAPS прямо на DC, я не буду устанавливать компонент AdmPwd GPO Extension – здесь он не нужен. В случае, если бы шла установка на обычную клиентскую ОС, развёрнутую на рабочей станции инженера, который будет заниматься LAPS, данный компонент бы понадобился, чтобы управлять паролем локального администратора на данной системе.



[Установка LAPS \(Local Administrator Password Solution\)](#)

[\(кликните для увеличения до 499 px на 385 px\)](#)

Компоненты, которые будут установлены:

- Fat Client UI – утилита для быстрого поиска рабочей станции или member server'a по имени и просмотра/смены информации по паролю учётной записи builtin-администратора
- PowerShell Module – подгружаемый модуль для выполнения административных задач LAPS через PowerShell
- GPO Editor templates – административные шаблоны для управления настройками модуля LAPS на клиентах

Далее установка тривиальна, а после неё я устанавливаю WMF 4.0 и можно переходить к подготовке Active Directory.

Расширяем схему для LAPS

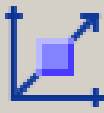
LAPS использует два дополнительных атрибута для хранения нужных данных – это `ms-Mcs-AdmPwd`, который используется для хранения пароля, и `ms-Mcs-AdmPwdExpirationTime`, в котором будет храниться время истечения действия пароля. Эти атрибуты добавляются просто – вам необходимо будет запустить PowerShell от учётной записи, имеющей права на модификацию схемы Active Directory (обычно это участник группы Schema Admins), и сделать два действия:

1. Подгрузить модуль LAPS – командлетом `Import-Module AdmPwd.PS`
2. Выполнить командлет `Update-AdmPwdADSchema`

По итогам этой операции в схеме Active Directory появятся два новых атрибута:

ms-Mcs-AdmPwd Properties

General

 ms-Mcs-AdmPwd

Description:

Common Name:

X.500 OID:

Syntax and Range

Syntax:

Minimum:

Maximum:

This attribute is single-valued.

☒ Atttribute is active

☐ Index this attribute

☐ Ambiguous Name Resolution (ANR)

☐ Replicate this attribute to the Global Catalog

☐ Attribute is copied when duplicating a user


☐ Index this attribute for containerized searches

[Атрибут ms-Mcs-AdmPwd, добавленный LAPS \(Local Administrator Password Solution\)](#)
(кликните для увеличения до 404 px на 443 px)

и

ms-Mcs-AdmPwdExpirationTime Properties ? X

General

 ms-Mcs-AdmPwdExpirationTime

Description:

Common Name: ms-Mcs-AdmPwdExpirationTime

X.500 OID: 1.2.840.113556.1.8000.2554.50051.45980.28111

Syntax and Range

Syntax: Large Integer/Interval

Minimum:

Maximum:

This attribute is single-valued.

☒ Attribute is active

☐ Index this attribute

☐ Ambiguous Name Resolution (ANR)

☐ Replicate this attribute to the Global Catalog

☐ Attribute is copied when duplicating a user

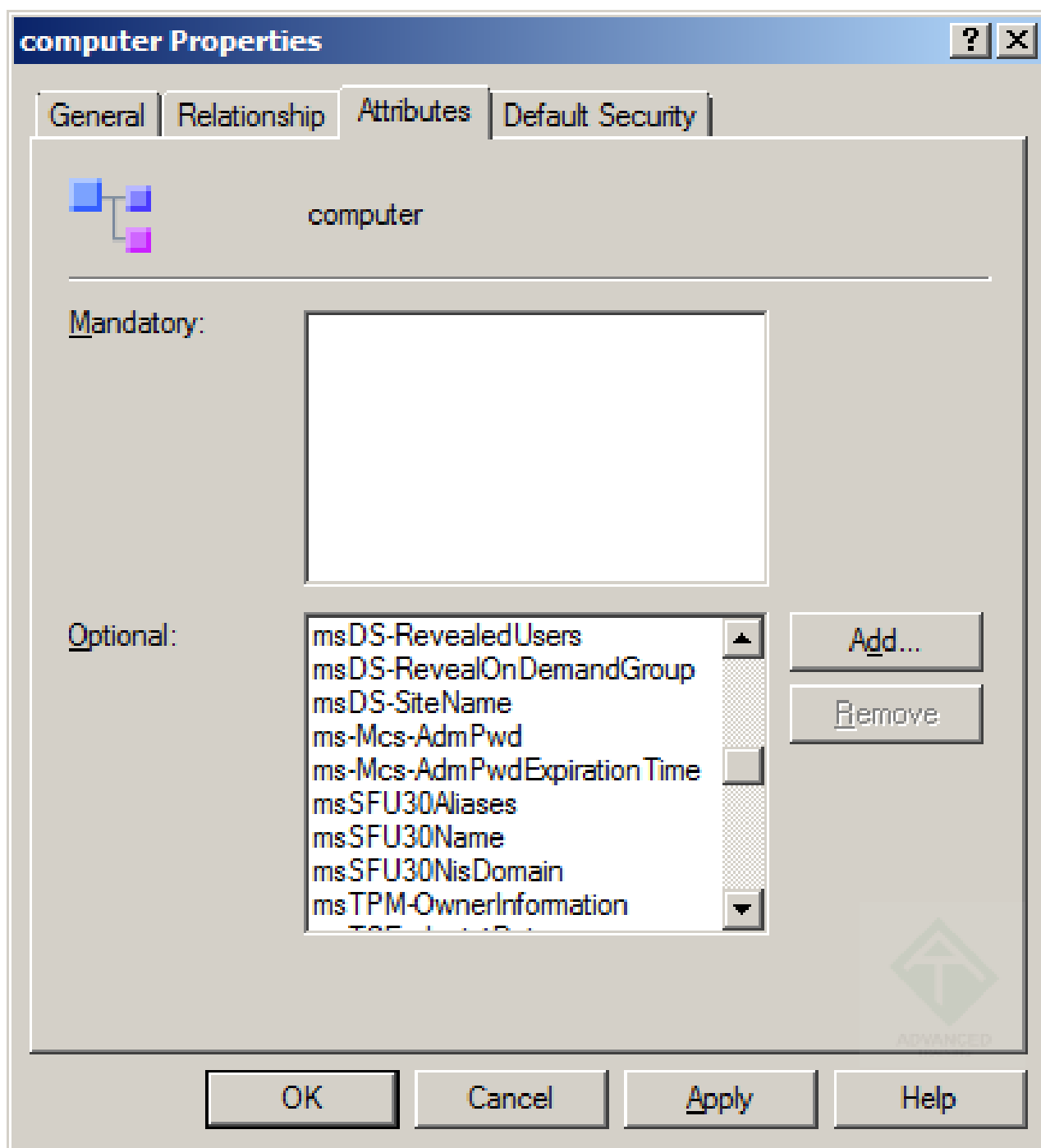
☐ Index this attribute for containerized searches

OK Cancel Apply Help

[Атрибут ms-Mcs-AdmPwdExpirationTime, добавленный LAPS \(Local Administrator Password Solution\)](#)

[\(кликните для увеличения до 404 px на 443 px\)](#)

Как видно, они простые в плане используемых типов и настроек – индексация на GC отключена (включать её не надо, вам же не нужна возможность поиска по тексту паролей, которые хранятся в открытом виде). Также можно увидеть, что данные атрибуты добавлены к классу computer:



[Атрибуты ms-Mcs-AdmPwd и ms-Mcs-AdmPwdExpirationTime, добавленные LAPS \(Local Administrator Password Solution\) к классу computer \(кликните для увеличения до 404 px на 443 px\)](#)

Подготовка схемы завершена – ну, разве что можете дописать комментарии к этим атрибутам, но это уже никак не повлияет на работу.

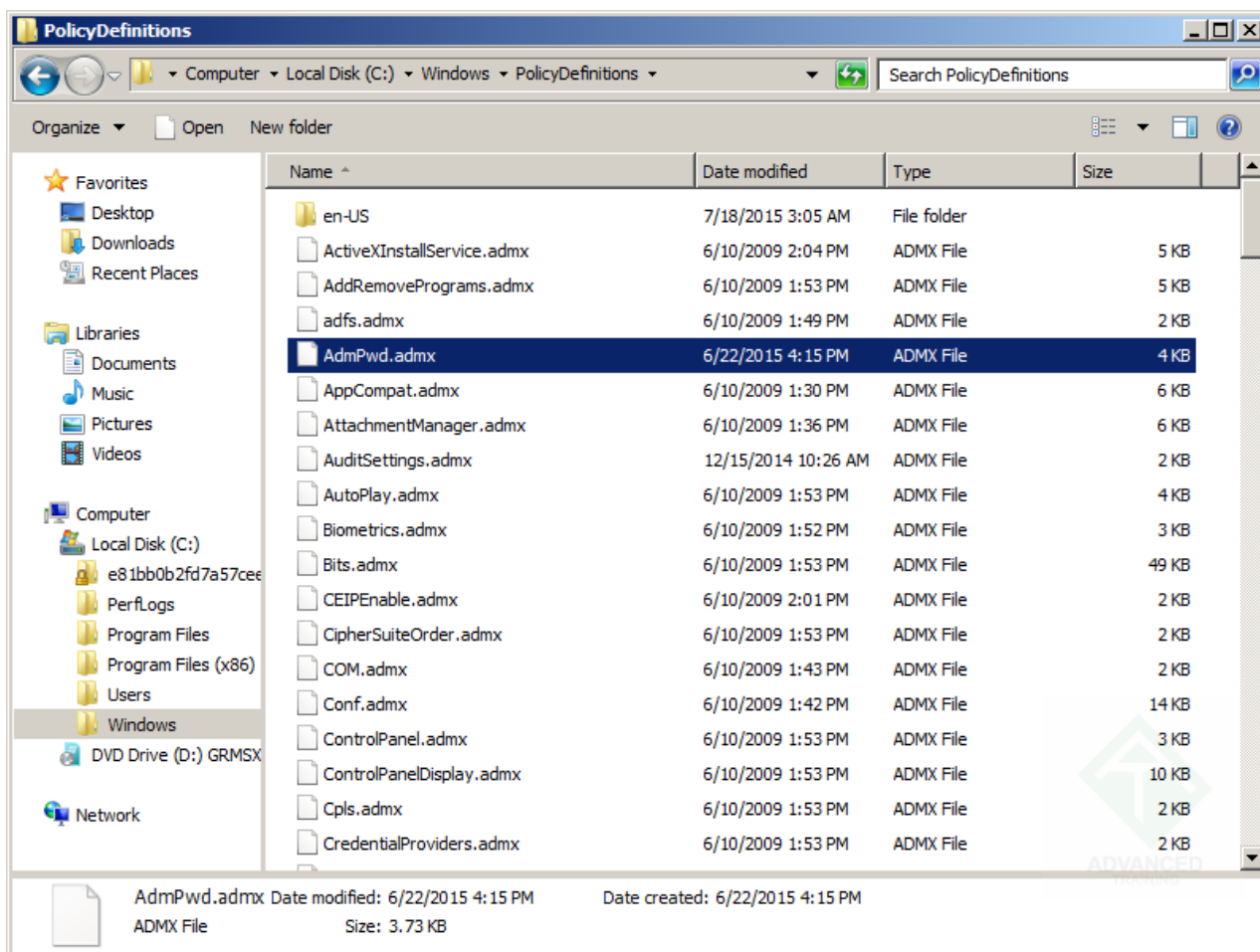
Теперь, после завершения подготовки леса Active Directory, перейдём к подготовке на уровне домена.

Подготовка домена для LAPS GPO

LAPS, для управления настройками на конкретных рабочих станциях/серверах или их группах устанавливает свои GPT (Group Policy Template). Он устанавливает их в свой каталог – чтобы они стали доступны сразу во всём домене, вынесем их в

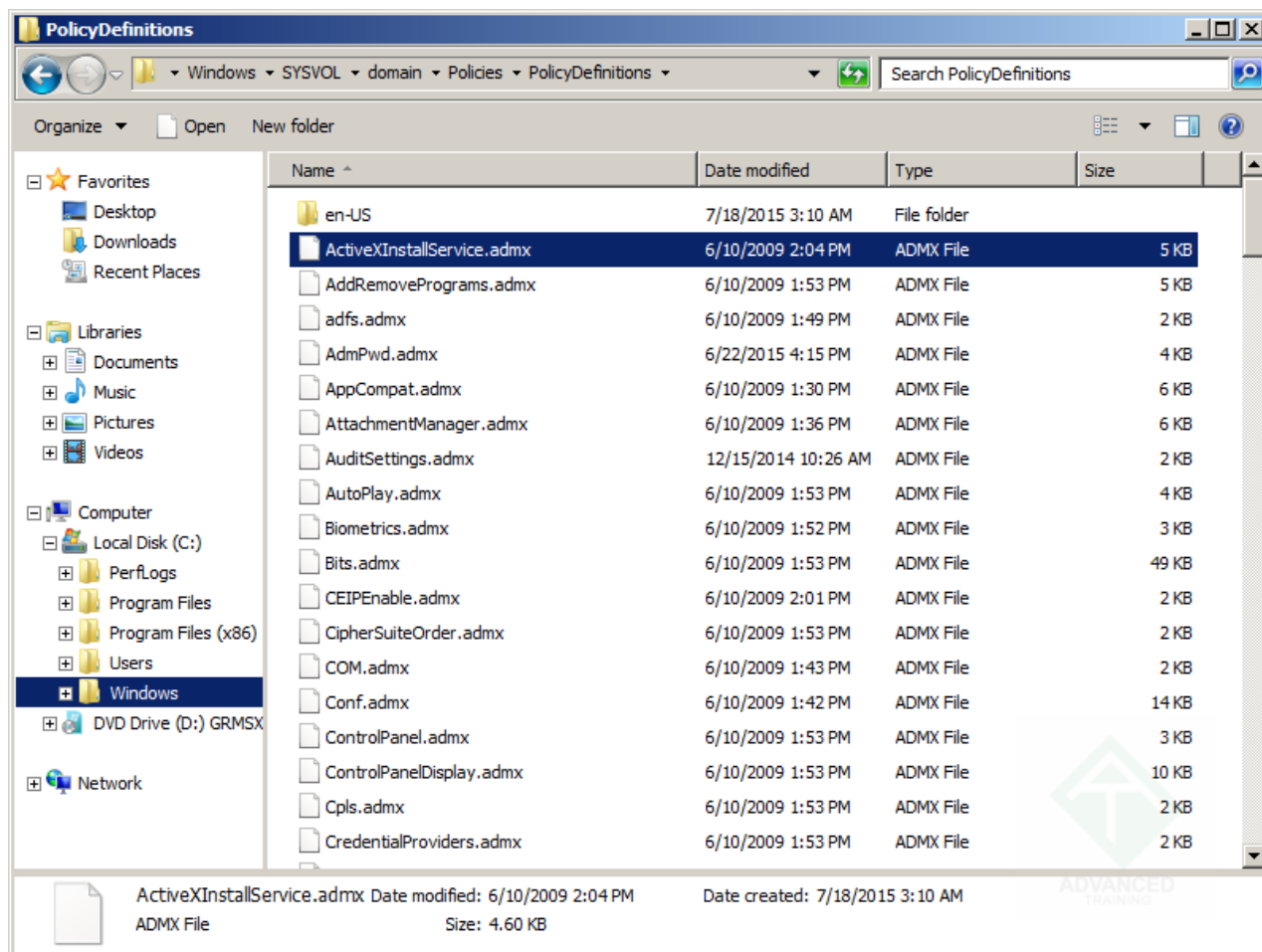
Central Storage – чтобы любой администратор, который может редактировать групповые политики, с любой точки домена видел эти настройки. Microsoft в официальной документации предлагает просто бросить эти шаблоны там, куда их по дефолту кидает инсталлятор – это неправильный шаг, не имеет смысла не пользоваться централизованным хранилищем Central Storage, оно лишь упрощает административные задачи. Мы сделаем правильно.

Находим шаблоны LAPS GPT:



[Шаблоны групповых политик для LAPS \(Local Administrator Password Solution\)](#)
(кликните для увеличения до 800 px на 600 px)

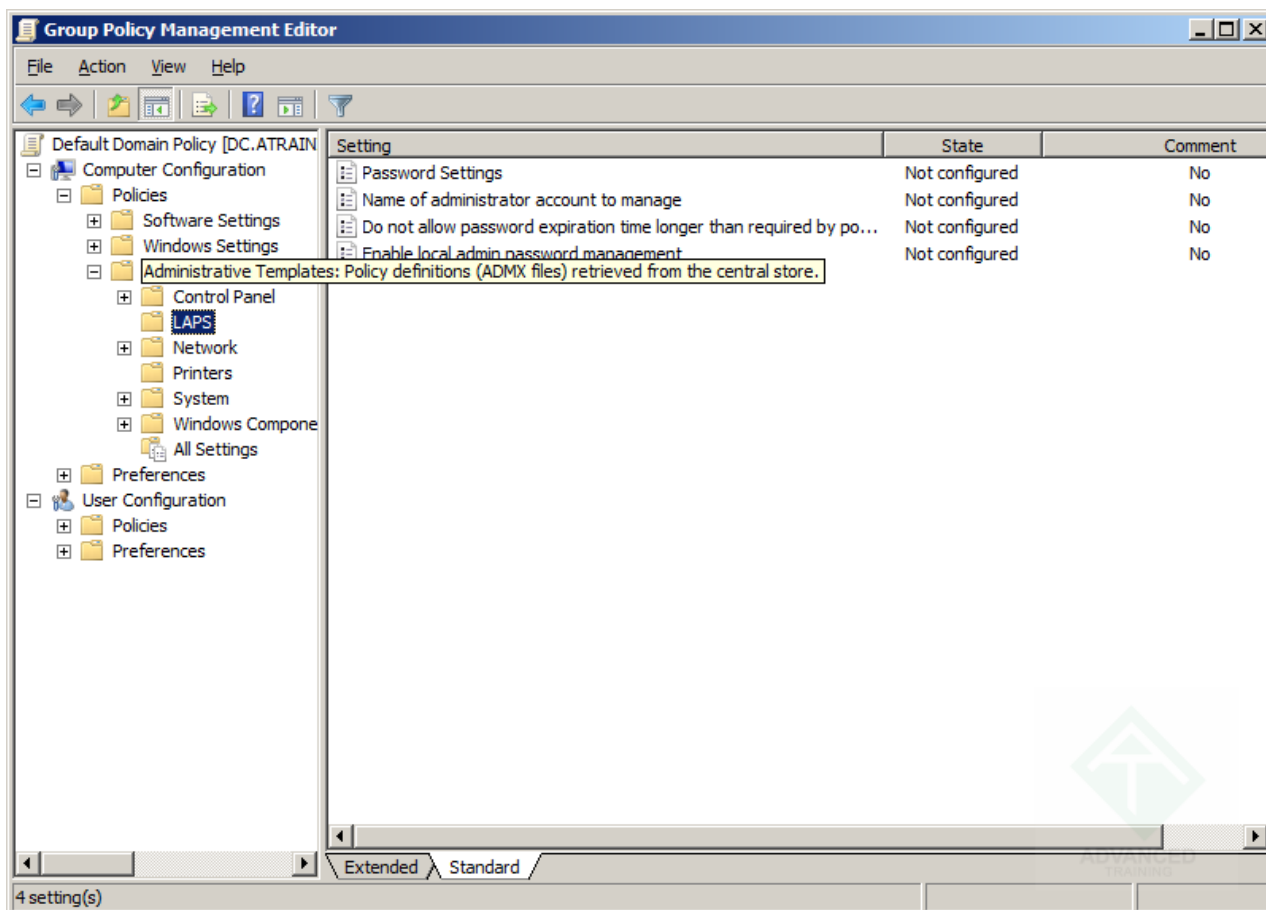
Не забудем, что нужен ещё и языковой файл – который AdmPwd.adml и лежит в подпапке en-us. Переносим их оба, сохраняя структуру хранения, в центральное хранилище политик нашего домена:



[Central Store для домена, в котором используется LAPS \(Local Administrator Password Solution\)](#)

[\(кликните для увеличения до 800 px на 600 px\)](#)

И проверяем, что всё корректно работает:



[Использование политик LAPS из Central Store](#)
(кликните для увеличения до 801 px на 572 px)

ОК, вопрос с политиками решили. Перейдём к специфике работы с RODC.

Подготовка для работы с LAPS RODC

Начиная с Windows Server 2008 у нас есть Read-only DC – специальный вариант контроллера домена, применяемый для региональных офисов и прочих мест, где контроля мало, а DC нужен. Ключевая специфика RODC будет в том, что он держит на себе копии разделов Active Directory, но не может в них писать (поэтому с него и репликация не нужна, ничего нового на нём появиться не может), но копии эти не только read-only – они ещё и не полные. В них отсутствует та информация, которую небезопасно держать в месте, куда возможен НСД. Изначально к этой информации относится достаточно очевидный комплект данных – например, пароли учётных записей, входящие в явно указанные группы. Но список не ограничивается паролями – также в него входят некоторые данные PKI, Bitlocker, а в нашем случае, раз мы начали использовать LAPS, этот комплект будет расширен автоматически. Ведь логично, что если мы боимся хранить на RODC хэши паролей, то реплицировать туда пароли локальных администраторов в открытом виде как-то странно.

Давайте убедимся, что всё ОК. Для этого откроем ADSI и зацепимся за раздел схемы:

Connection Settings [X]

Name: Schema

Path: LDAP://dc.atraining.lab/Schema

Connection Point

☐ Select or type a Distinguished Name or Naming Context:

☐ Select a well known Naming Context:

Schema

Computer

☐ Select or type a domain or server: (Server | Domain [:port])

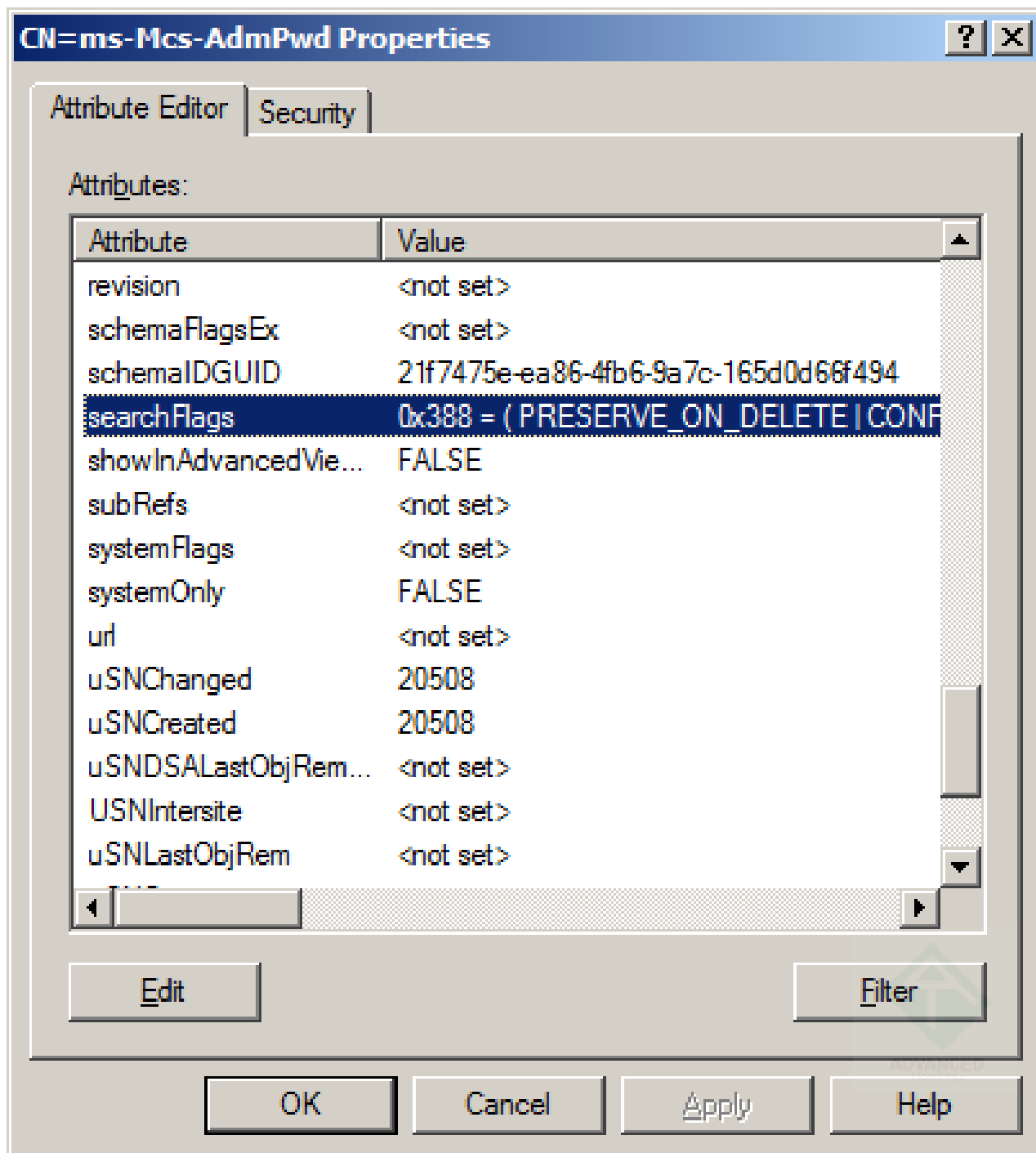
☒ Default (Domain or server that you logged in to)

☐ Use SSL-based Encryption

Advanced... OK Cancel

[Просмотр изменений в schema partition](#)
(кликните для увеличения до 384 px на 379 px)

А после найдём атрибут ms-Mcs-AdmPwd:



[Просмотр изменений в schema partition](#)

([кликните для увеличения до 404 px](#) на [448 px](#))

Нас будет интересовать значение атрибута searchFlags – это битовый массив, указывающий, как обращаться с данным атрибутом – искать ли по его значению, передавать в GC, и реплицировать ли на RODC. В нашем случае значение по умолчанию будет 0x388 – это сумма флагов PRESERVE_ON_DELETE, CONFIDENTIAL, NEVER_AUDIT_VALUE, RODC_FILTERED. Мы видим, что нужные нам атрибуты – CONFIDENTIAL (это 7й бит) и RODC_FILTERED (это 10й) выставлены правильно, т.е. доступ к атрибуту будет ограничен и реплицироваться на RODC он не будет. Всё ОК. Кстати, как понятно, Вы можете аналогичным образом защитить любой нужный атрибут, который не нужен на RODC – допустим, какой-то добавленный Вами вручную и содержащий приватную информацию. Атрибут будет по прежнему

доступен, но не будет храниться на RODC – поэтому злонамеренные товарищи, ночью выкрутившие жёсткий диск из RODC и сделавшие его полную копию, при просмотре ntds.dit ничего не увидят.

ОК, теперь перейдём к защите наших данных от тех пользователей Active Directory, которым необязательно знать пароли локальных администраторов на разных рабочих станциях и серверах.

Защищаем хранение паролей в Active Directory

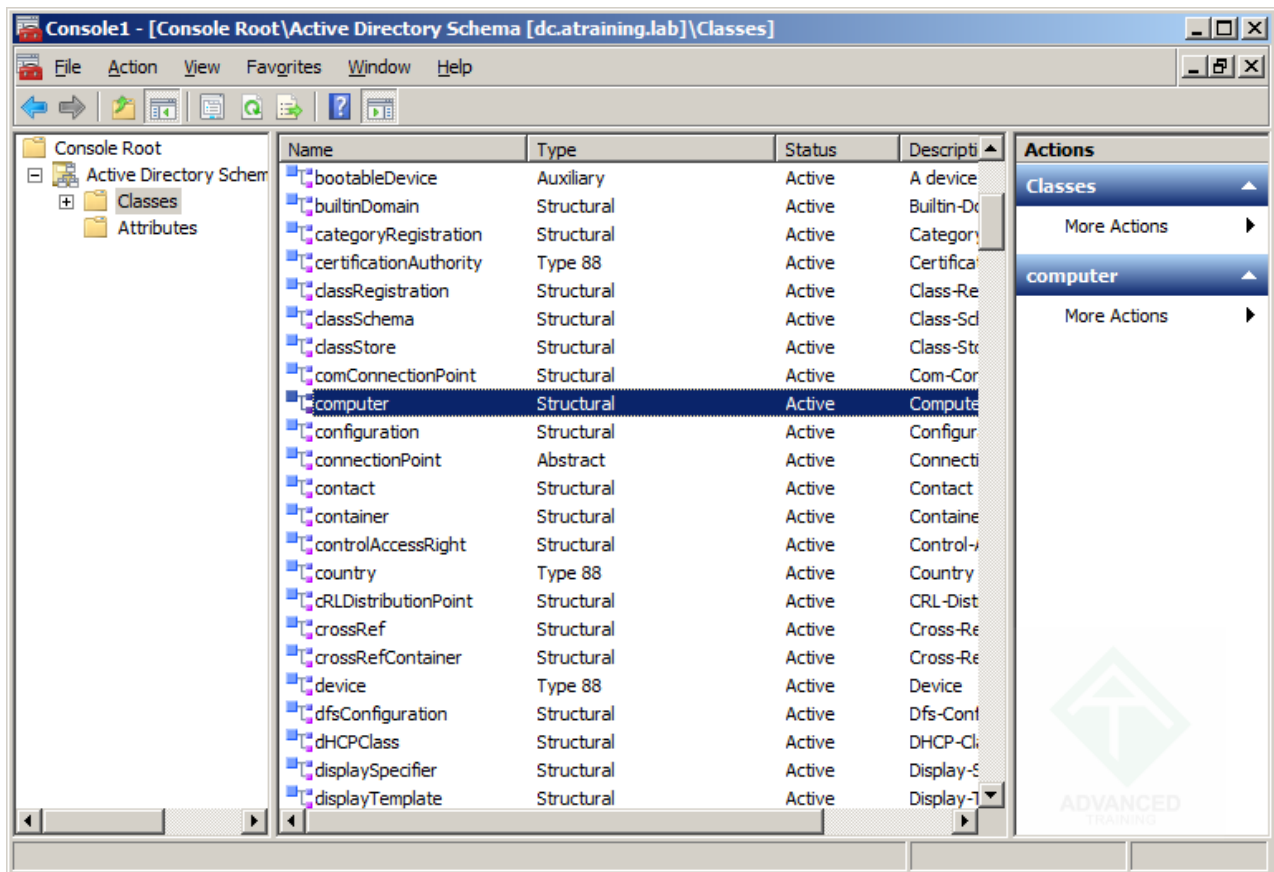
Мы добавили новый атрибут – и он, как положено, доступен каждому на чтение. У всех пользователей есть право Read All Properties – так повелось с древних времён, когда ещё были гибридные структуры Active Directory + NT 4.0. Microsoft предлагает самурайский способ – запретить всем пользователям читать все расширенные атрибуты. Вообще. Что ж, вариант фиговый – из-за установки одной административной утилиты, не глядя на другое использующееся ПО, глобально зарубить всё. Это неправильно, мы сделаем тоньше – запретим целевым security principal'ам только чтение и запись данных атрибутов, не затрагивая другие.

Для этого создаём группу с очевидным названием (вы, конечно, придумаете более благозвучное и в стиле локальной системы именования групп в вашем домене):

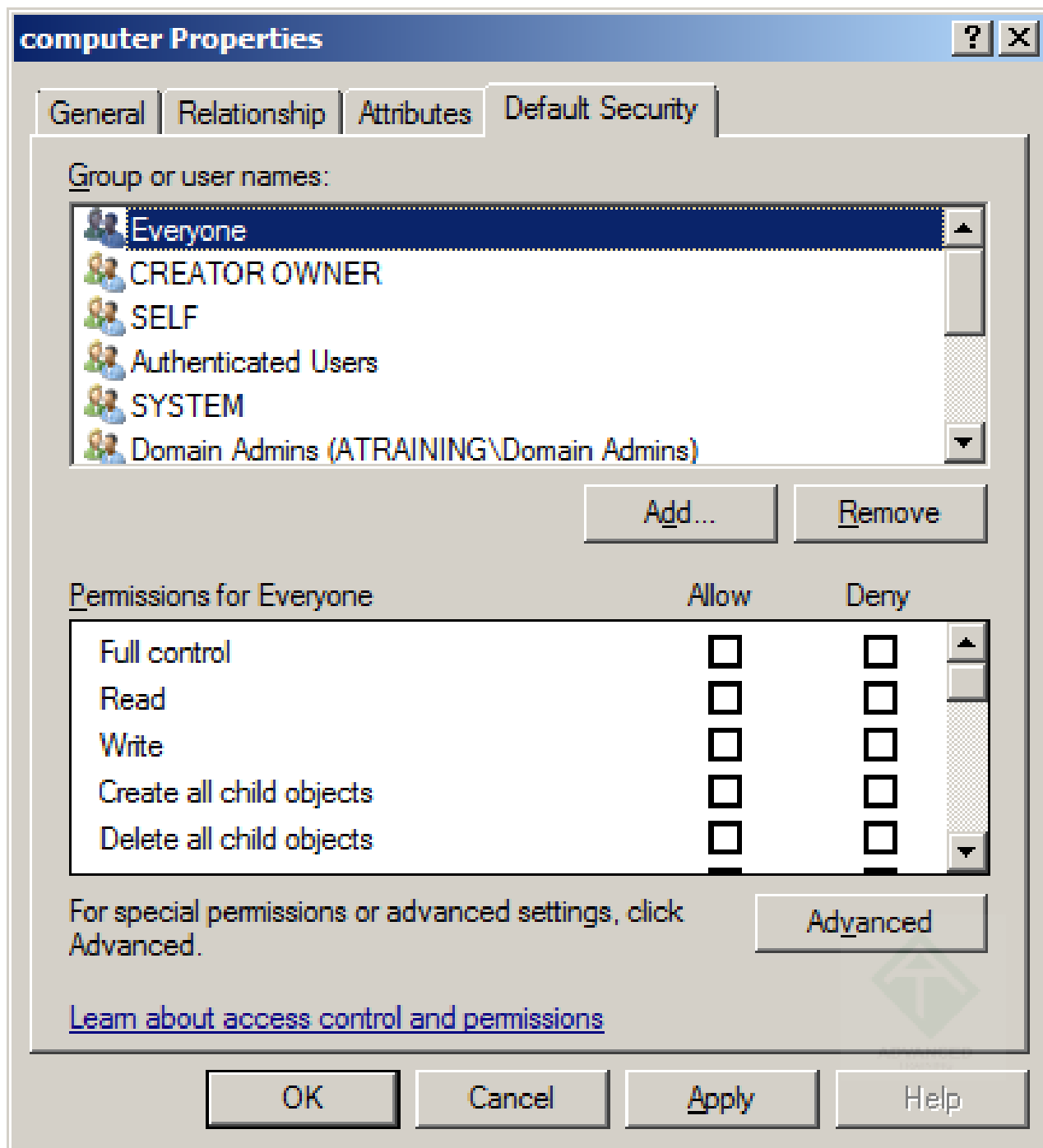
The screenshot shows a Windows XP-style dialog box titled "No local admin password access Properties". It has four tabs: "Object", "Security", "Attribute Editor", and "General". The "General" tab is active, displaying a group icon and the name "No local admin password access". Below this, there are input fields for "Group name (pre-Windows 2000):", "Description:", and "E-mail:". The "Group scope" section has three radio buttons: "Domain local", "Global" (selected), and "Universal". The "Group type" section has two radio buttons: "Security" (selected) and "Distribution". At the bottom is a large "Notes:" text area. The dialog box has "OK", "Cancel", "Apply", and "Help" buttons at the bottom.

[Создаём в Active Directory группу, которой запретим просмотр и изменение паролей локальных учётных записей администраторов \(кликните для увеличения до 404 px на 466 px\)](#)

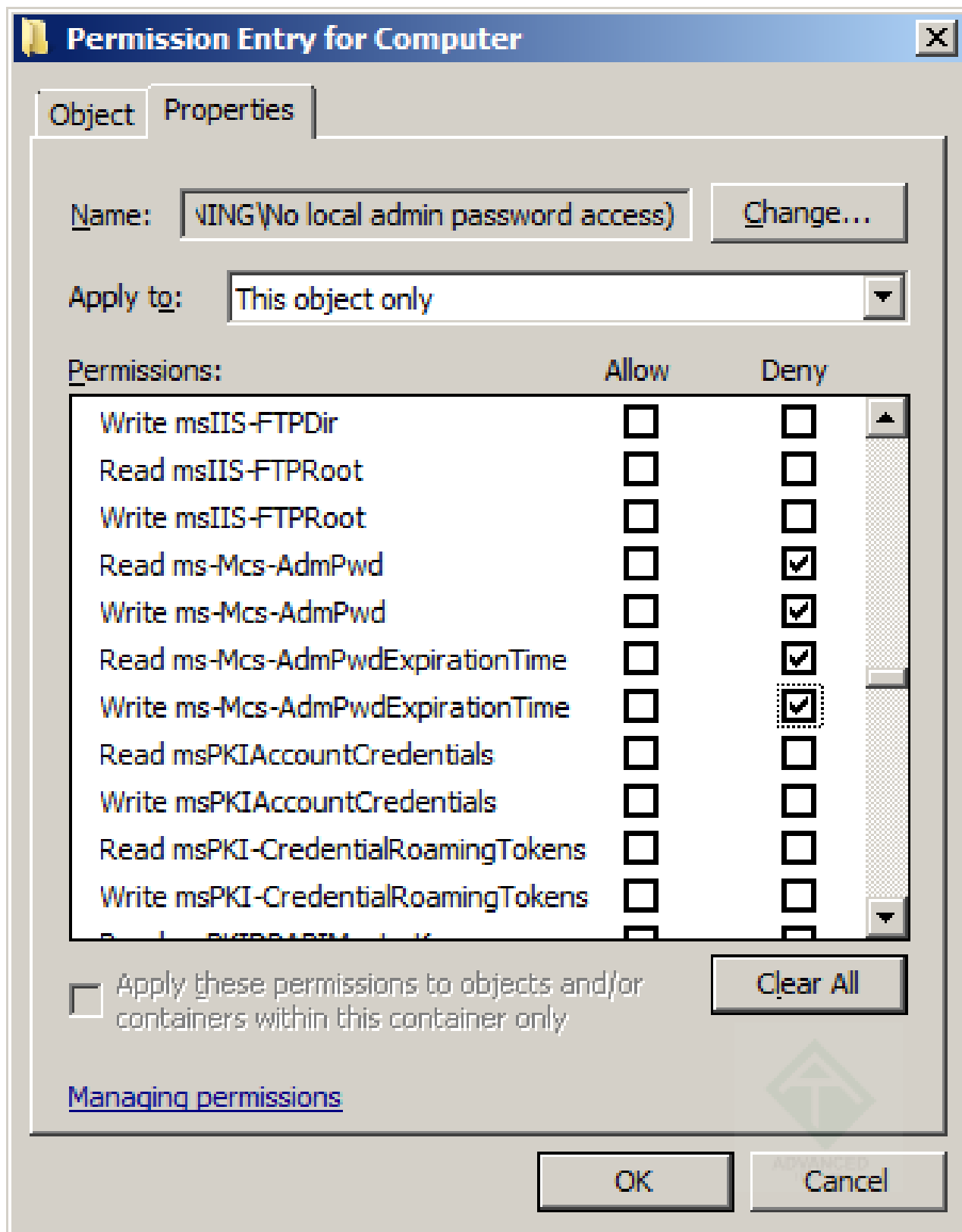
В эту группу вы после добавите тех участников, которым в явном виде не нужно работать с данными о паролях администраторов – например, используя группы сотрудников по отделам, или как-то ещё – зависит от вашей Active Directory. Теперь укажем, что на новорожденных учётных записях компьютеров эта группа сразу имеет данный запрет, для этого откроем редактор схемы (у кого в mmc / Add Snap-Ins его нет – просто выполните от локального администратора команду `regsvr32 schmmgmt.dll`) и выберем Default ACL у объекта computer:



[Редатируем в Active Directory schema объект computer](#)
(кликните для увеличения до 768 px на 525 px)



[Редактируем в Active Directory schema ACL объекта computer](#)
(кликните для увеличения до 404 px на 443 px)



[Редактируем в Active Directory schema отдельную ACE объекта computer \(кликните для увеличения до 367 px на 468 px\)](#)

Не забудьте снять все прочие разрешения у данной группы – это кнопкой Clear All на первой и на второй вкладках. Соответственно, если хотите ещё более гранулярную раздачу прав на атрибуты – можете сделать две группы, одной запретить просмотр, а другой, например, запись. По аналогии.

На уже существующих учётных записях рабочих станций и серверов надо также будет выставить эту ACE – как это сделать, выбирайте сами – или, если у вас хорошо прописанная структура OU в Active Directory, просто унаследовать её на определённый тип объектов с корневых контейнеров, или как-то ещё. Ключевое в этой задаче – обычный пользователь, имеющий стандартные права на чтение всех объектов, не должен иметь возможность читать данный атрибут.

Теперь выдадим компьютерной учётной записи нужные для реализации механизма LAPS права на саму себя. Это нужно затем, чтобы работающий от локальной системной учётной записи сервис, который сработает на применении групповой политики, смог бы работать с парольными атрибутами в Active Directory. Так как локальный сервис будет имперсонироваться в учётную запись рабочей станции / сервера в Active Directory, то нам надо будет в том же редакторе схемы найти ACE про SELF и там добавить право на работу с данными атрибутами:

Permission Entry for Computer

Object Properties

Name: SELF Change...

Apply to: This object only

Permissions:	Allow	Deny
Write msIIS-FTPRoot	<input type="checkbox"/>	<input type="checkbox"/>
Read ms-Mcs-AdmPwd	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write ms-Mcs-AdmPwd	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read ms-Mcs-AdmPwdExpirationTime	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write ms-Mcs-AdmPwdExpirationTime	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read msPKIAccountCredentials	<input type="checkbox"/>	<input type="checkbox"/>
Write msPKIAccountCredentials	<input type="checkbox"/>	<input type="checkbox"/>
Read msPKI-CredentialRoamingTokens	<input type="checkbox"/>	<input type="checkbox"/>
Write msPKI-CredentialRoamingTokens	<input type="checkbox"/>	<input type="checkbox"/>
Read msPKIDPAPIMasterKeys	<input type="checkbox"/>	<input type="checkbox"/>
Write msPKIDPAPIMasterKeys	<input type="checkbox"/>	<input type="checkbox"/>
Read msPKIRoamingTimeStamp	<input type="checkbox"/>	<input type="checkbox"/>

☐ Apply these permissions to objects and/or containers within this container only

[Managing permissions](#)

Clear All

OK Cancel

[Добавляем в Active Directory schema права на модификацию атрибутов LAPS для объекта computer](#)

(кликните для увеличения до 367 px на 468 px)

Опять-таки – то же самое нужно проделать со всеми уже существующими учётными записями компьютеров/рабочих станций – LAPS в этом плане может предложить лишь частичную автоматизацию путём запуска на контейнере с компьютерами командлета `Set-AdmPwdComputerSelfPermission -OrgUnit имя_контейнера`, который

добавит данную строчку и включит её наследование на нужный тип child object'ов. Как именно вы это сделаете – некритично, цель – разрешить компьютеру от себя лично работать с данными атрибутами своей же учётки в Active Directory.

Следующий шаг – раздать права тем, кто будет администрировать эти пароли локальных администраторов. А то мы пользователям обычным доступ выключили, компьютерам для применения политик включили, а бедный админ, поставивший GUI-клиента LAPS, остался в стороне.

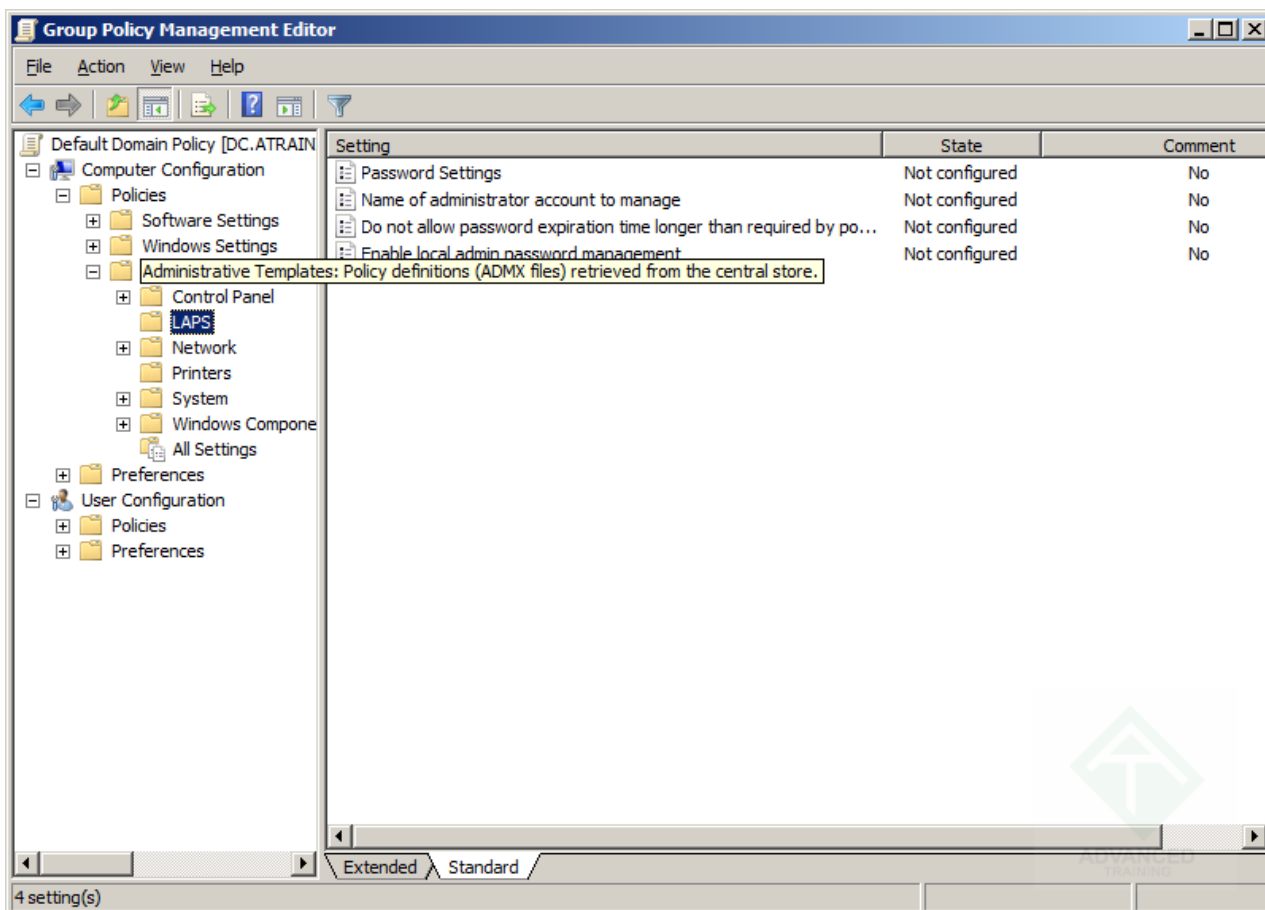
Снова действуем по аналогии – создаём группу с именем вида “Builtin Administrators password management”, добавляем в неё нужных участников и выдаём этой группе право на доступ к атрибуту с паролем – который `ms-Mcs-AdmPwd`. Скриншоты не делаю, т.к. всё абсолютно по аналогии с предыдущими действиями – и в PowerShell-модуле LAPS опять же есть на этот счёт командлет, упрощающий работу: `Set-AdmPwdReadPasswordPermission -OrgUnit контейнер_в_котором_компьютеры -AllowedPrincipals наша_группа_тех_кто_имеет_право_сбрасывать_на_этих_компьютерах_пароль_локального_админа`. Как и в предыдущих действиях – не забудьте, пожалуйста, добавить эти же права в Default ACL компьютерной учётной записи – Microsoft это забывает сделать.

Для второго атрибута – который `ms-Mcs-AdmPwdExpirationTime` – делаем аналогичное действие, права на него нужны тем, кто будет сбрасывать пароли (по сути, этот процесс будет состоять в изменении срока действия, чтобы система сама изменила пароль). Командлет будет чуть другой по названию – `Set-AdmPwdResetPasswordPermission`, параметры у него будут те же.

В общем всё – теперь перейдём к настройке политик.

Настраиваем политики LAPS для рабочих станций и member-серверов

Политик немного, всего 4, пробежимся по ним, т.к. не все они очевидны в плане настроек.



[Использование политик LAPS из Central Store](#)
(кликните для увеличения до 801 px на 572 px)

Enable local admin password management

Это – включение локального клиента LAPS, являющегося CSE. Тут всё просто – если не включен, но установлен, то работать не будет – надо и установить, и включить.

Password Settings

Настройки сложности пароля и времени автоматической замены. В общем, тут ничего волшебного – всё это же есть и при работе с обычными паролями.

Name of administrator account to manage

Здесь уже интереснее. Если вы используете LAPS для управления учёткой встроенного админа – то этот параметр вам не пригодится, система сама поймёт, про что речь. Но LAPS может также использоваться и для управления другими учётными записями с правами локального администратора. То есть вы можете, например, через стандартные политики переименовать встроенного админа на всех серверах и рабочих станциях, выдать ему разово какой-нибудь специфичный пароль символов в 40, а потом его выключить – и после завести другую учётку для локального администрирования, и вот уже ей раздавать пароль через LAPS. Это неплохой вариант, поскольку всё же права встроенной учётки администратора чуть

выше, чем произвольной из группы BUILTIN\Administrators – и создание специфичной не-встроенной учётки локального админа – хороший ход с точки зрения безопасности.

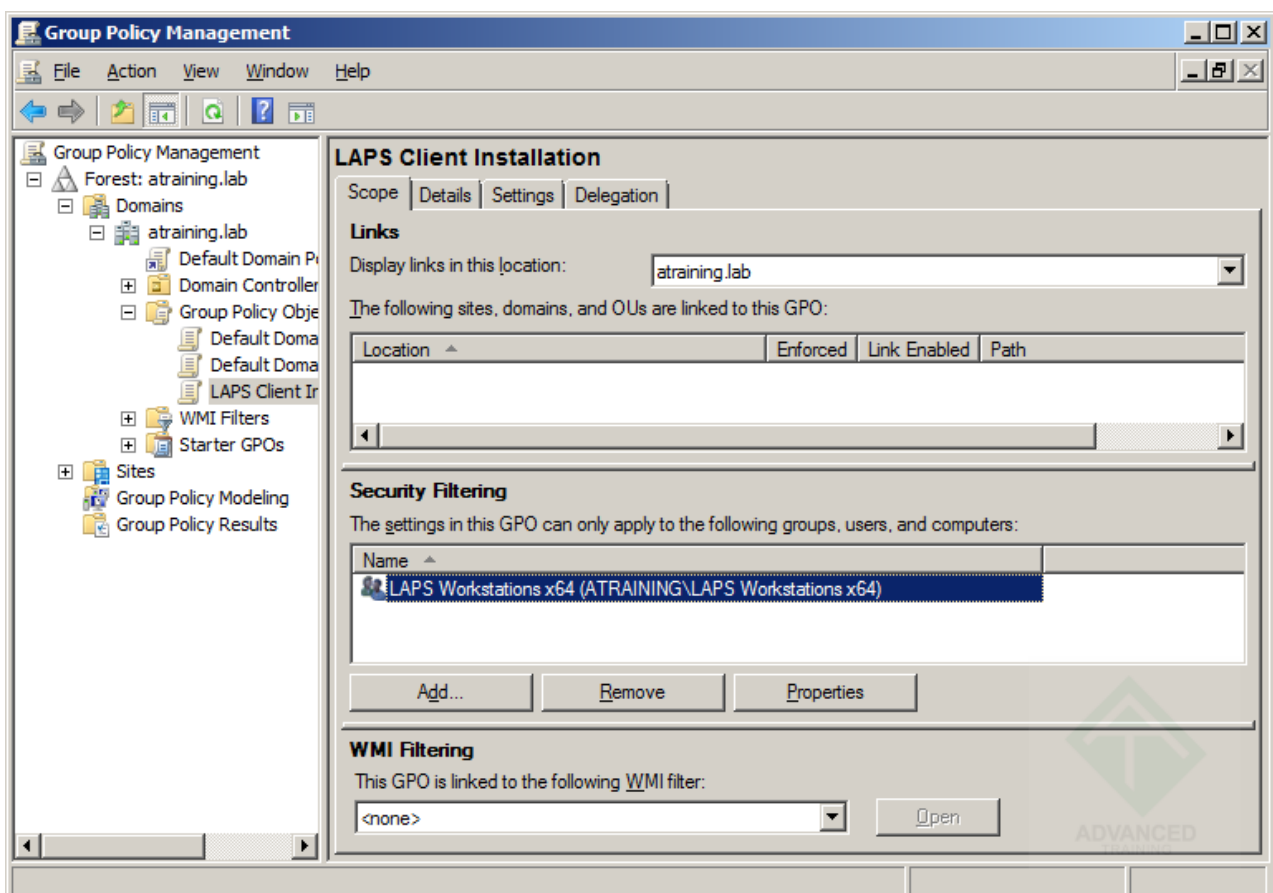
Do not allow password expiration time longer than required by policy

Это специфичная настройка, нужная для разрешения конфликта – когда в Password Settings установлено одно время смены пароля, а вручную в атрибуте `ms-Mcs-AdmPwdExpirationTime` – другое. Если эту настройку включить, пароль будет автоматически сменён в случае наступления любого из этих двух сроков – искусственно продлить время жизни не получится.

Ну а теперь, в принципе, самое простое – развёртывание клиента LAPS.

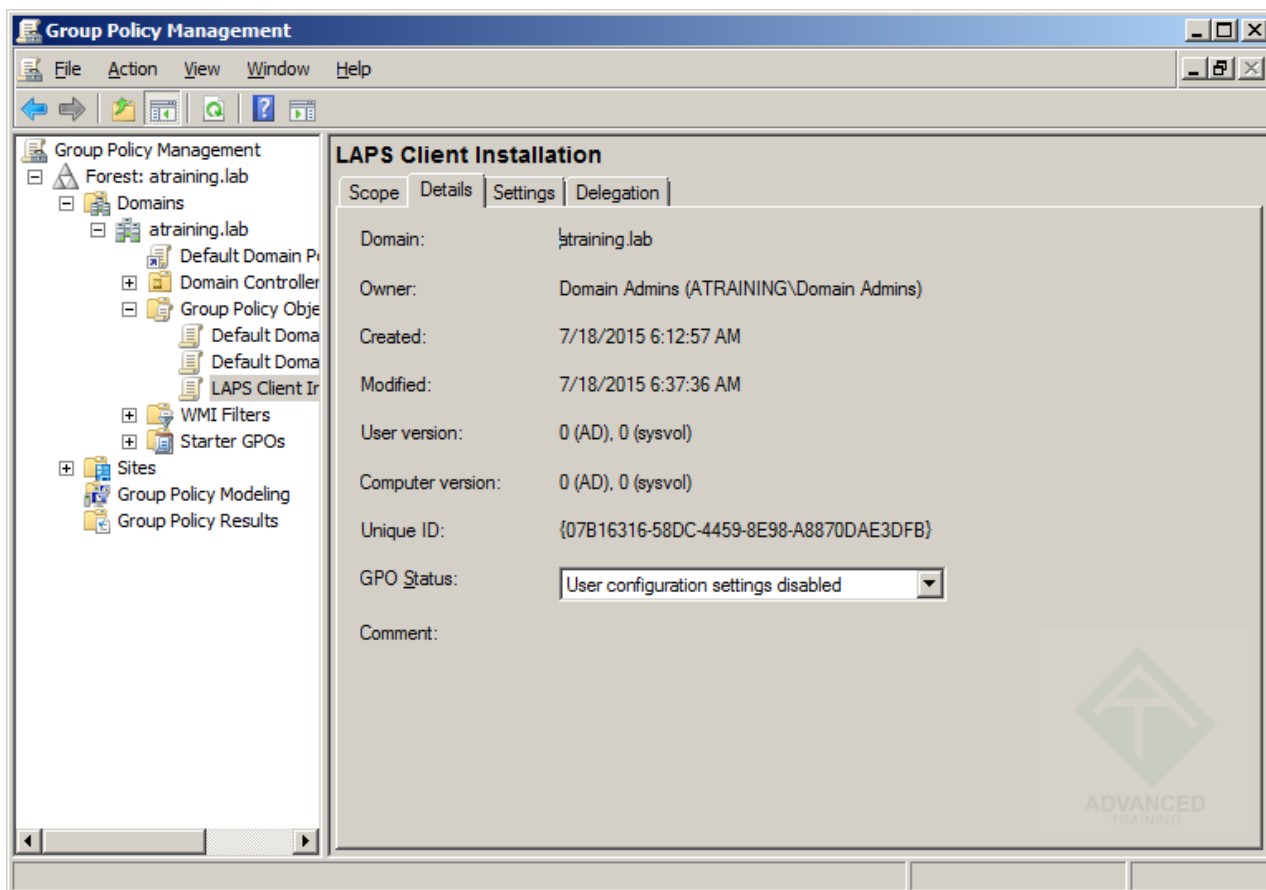
Развёртываем LAPS для клиентов – рабочих станций и member-серверов

Это несложно и не требует дополнительного ПО – всё, что нужно – создать новую групповую политику, добавить в неё MSI-модуль LAPS (учитывая битовость целевых систем), назначить его установку от имени компьютера, и нацелить эту политику на нужную группу хостов. Выглядеть это будет примерно так:



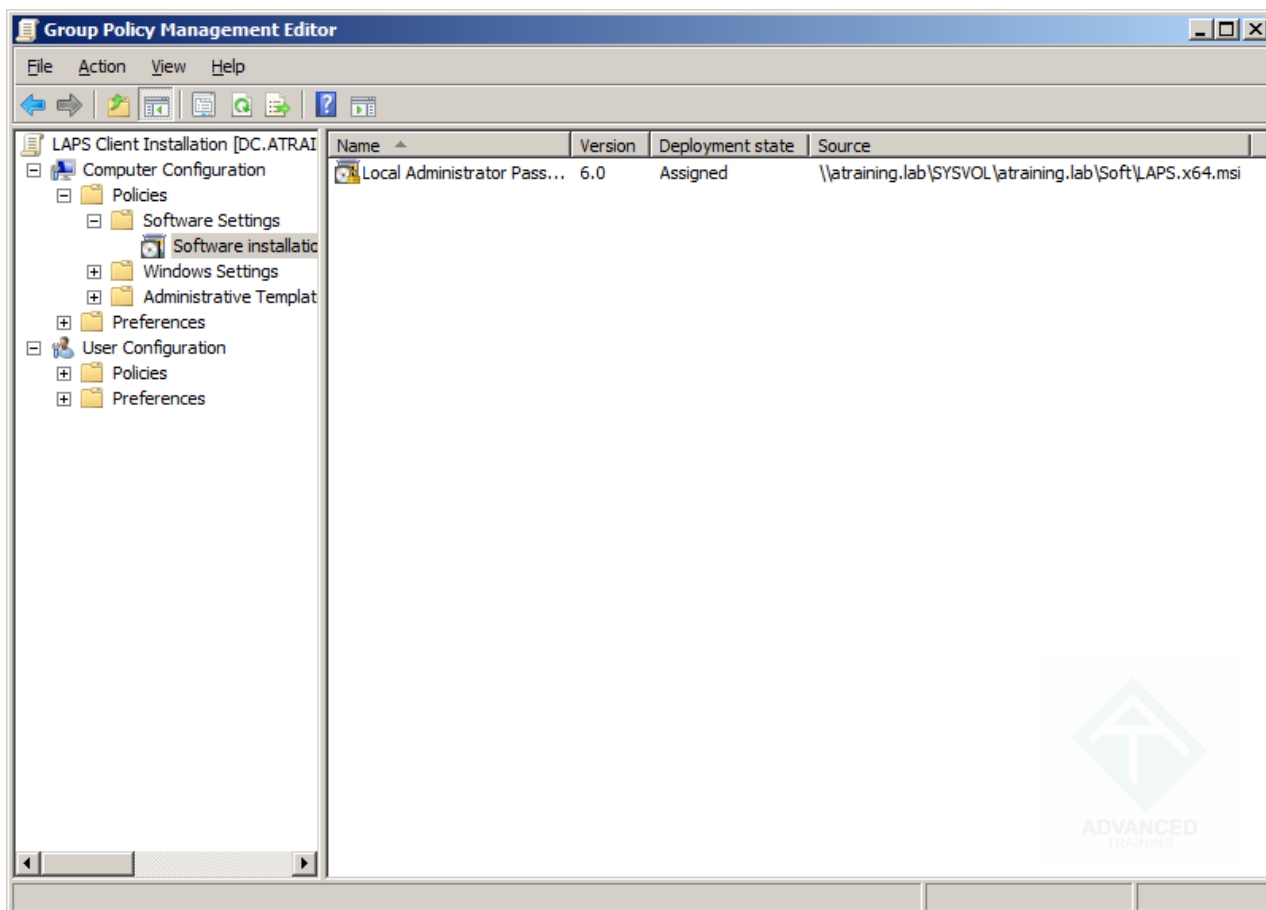
[Создание групповой политики для установки клиентской части LAPS](#)
(кликните для увеличения до 768 px на 537 px)

Отключаем для ускорения применения юзерскую часть – там настроек все равно нет:



[Создание групповой политики для установки клиентской части LAPS - отключаем обработку половинки для user accounts \(кликните для увеличения до 768 px на 537 px\)](#)

Выкладываем msi-файлы для LAPS на общедоступный сетевой ресурс, чтобы клиенты могли их оттуда забирать – я выложу прямо в SYSVOL, предполагая, что данная утилита будет использоваться по всей организации – вы же можете сделать отдельную distribution point с использованием DFS и адресно прописать и схему репликации, и потребление полосы пропускания, и всё другое нужное и необходимое – а после выкладывания назначаем (Assign) на раздачу для компьютеров, подпавших под эту политику:



[Создание групповой политики для установки клиентской части LAPS - раздаём LAPS \(кликните для увеличения до 801 px на 572 px\)](#)

Можно и более автоматизированно – добавить в политику WMI-фильтр, который ограничит её применение 64х битовыми системами:

Only x86-64 hosts [X]

Name:

Description:

Queries:

Namespace	Query
root\CIMv2	select * from Win32_OperatingSystem WHERE OSArchitecture = "64-bit"

[Создание WMI-фильтра для ограничения применения групповой политики установки клиентской части LAPS](#)

[\(кликните для увеличения до 476 px на 340 px\)](#)

Замечу, что атрибут OSArchitecture класса Win32_OperatingSystem будет только у NT 6.0 и выше – однако, системы на базе Windows XP мы не учитываем; если же нужно устанавливать LAPS на много разных Windows Server 2003, которые NT 5.2 и могут быть и x86, и x86-64, то можно воспользоваться анализом атрибута AddressWidth у класса Win32_Processor:

Only x86-64 hosts [X]

Name:
Only x86-64 hosts

Description:

Queries:

Namespace	Query
root\CIMv2	SELECT AddressWidth FROM Win32_Processor WHERE AddressWidth = '64'

Add
Remove
Edit

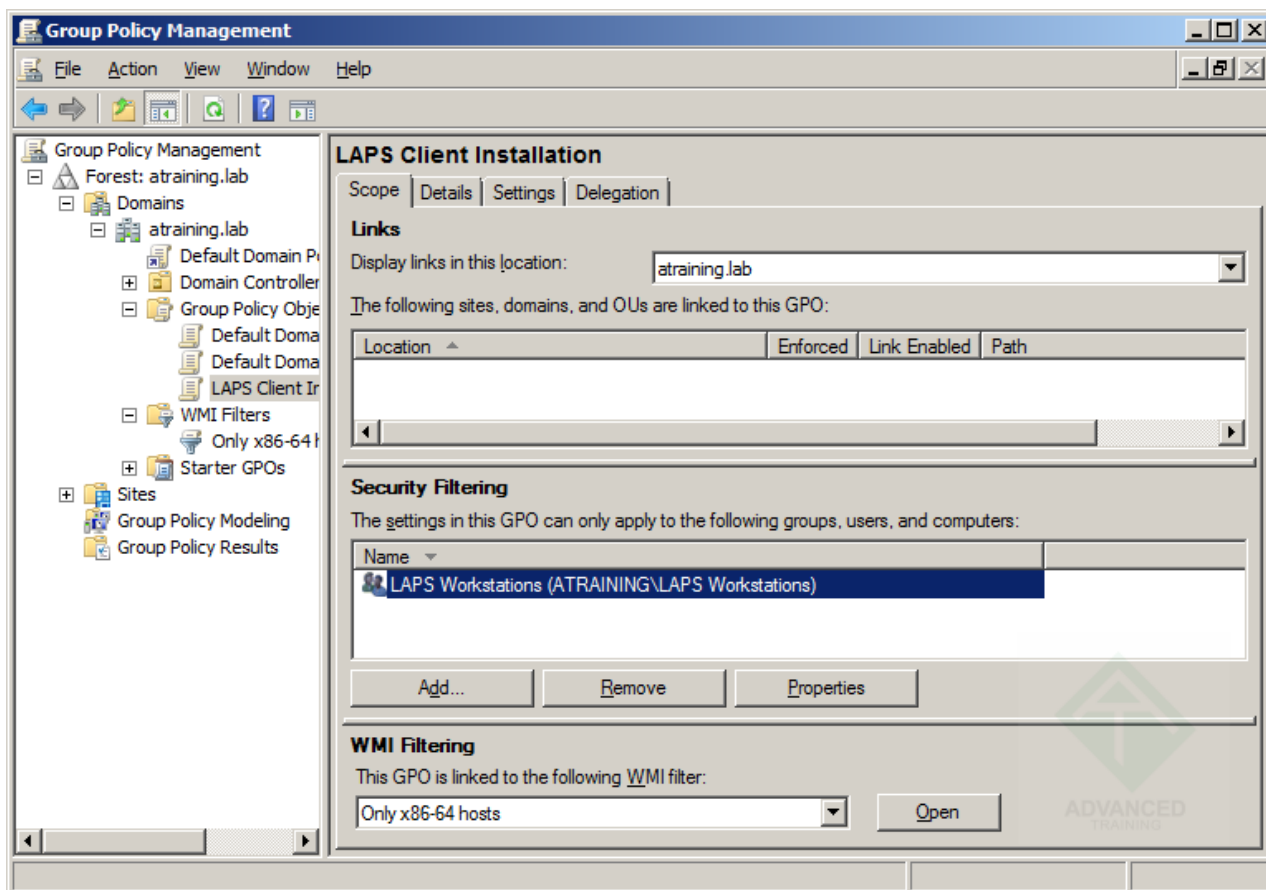
ADVANCED
[Up Arrow]

Save Cancel

[Создание WMI-фильтра для ограничения применения групповой политики установки клиентской части LAPS для Windows Server 2003](#)
([кликните для увеличения до 476 px на 340 px](#))

Это менее точный параметр, т.к. на систему с 64х битовым процессором может быть установлена 32х битовая ОС.

Вот так будет в результате выглядеть наша финальная политика:



[Создание групповой политики LAPS с WMI-фильтром](#) (кликните для увеличения до 768 px на 537 px)

В этом случае можно не заводить дополнительные группы вида “все 64х битовые хосты” / “все 32х битовые хосты”, а просто назначить обе политики – и для 32х, и для 64х битовых систем – на нужные контейнеры. Группа же LAPS Workstations служит дополнительным ограничением применения – в неё можно добавить, допустим, Domain Computers, в случае массового развёртывания, а можно и security-группы по отделам предприятия, например.

Вкратце всё. Теперь LAPS можно штатно использовать – после применения политик и установки модуля пароли автоматически сгенерятся и попадут в Active Directory. Как запустить утилиту администрирования (она установится и будет в меню) и нажимать там обе функциональные кнопки Set и Search – думаю, не требует доп. пояснений. :)

Напоследок

В итоге мы имеем хороший и надёжный механизм автоматизации одной из админских задач – потому что пароли локальных администраторов все равно есть и управлять ими как-то надо. Теперь это ощутимо проще и безопаснее.

Удачного применения!