Аннотация

Групповая политика применяется к пользователю или компьютеру в зависимости от того, где оба объекта располагаются в службе Active Directory. Однако в некоторых случаях пользователям может быть необходима применимая к ним политика на основе местоположения только объекта компьютера. Функцию замыкания групповой политики можно использовать для применения объектов групповой политики (GPO), зависящих только от того, на какой компьютер входит пользователь.

Дополнительная информация

Чтобы установить пользовательскую настройку для каждого компьютера, выполните следующие условия:

1. В оснастке «Групповая политика» консоли управления (ММС) выберите **Конфигурация компьютера**.
2. Найдите окно **Административные шаблоны**, выберите **Система** и**Групповая политика** и включите функцию**Режим обработки замыкания пользовательской групповой политики**.

Эта политика предписывает системе применить набор объектов GPO к любому пользователю, входящему на компьютер, управляемый этой политикой. Эта политика предназначена для специализированных компьютеров, где необходимо изменить политику пользователя на основе того, какой компьютер используется. Например, компьютеры в общественных местах, в лабораториях и учебных классах.  
  
**Примечание.** Функция замыкания политики поддерживается только в среде Active Directory. И учетная запись компьютера, и учетная запись пользователя должны быть в Active Directory. Если каждой учетной записью управляет контроллер домена на основе Microsoft Windows NT 4.0, функция замыкания политики не работает. Клиентский компьютер должен находиться под управлением одной из следующих операционных систем:

* Windows XP Professional
* Windows 2000 Professional
* Windows 2000 Server
* Windows 2000 Advanced Server
* Windows Server 2003

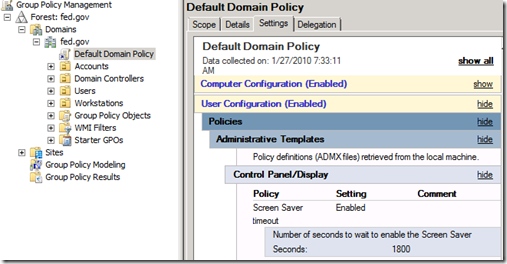
В то время как пользователи работают на своих рабочих станциях, может оказаться необходимым применить параметры групповой политики на основе местоположения объекта пользователя. В этом случае рекомендуется настраивать параметры политики на основе организационного подразделения, в котором находится учетная запись пользователя. Однако в некоторых случаях объект компьютера находится в конкретном огранизационном подразделении, и пользовательские параметры политики будут применяться согласно местоположению не объекта пользователя, а объекта компьютера.  
  
**Примечание** Невозможно выполнить фильтрацию параметров пользователя, которые были произведены посредством запрета или удаления AGP и прав на чтение из объекта компьютера, указанного для замыкания политики .   
  
Обычная обработка групповой политики пользователя указывает, что к компьютерам, расположенным в своем подразделении, применяются объекты групповой политики в порядке запуска компьютера. К пользователям в их подразделениях применяются объекты групповой политики в порядке входа в систему независимо от компьютера, за которым они работают.   
  
В некоторых случаях этот порядок обработки может быть другим. Например, если нежелательно, чтобы приложения, назначенные или опубликованные для пользователей в подразделении, были установлены в то время, как пользователь входит в систему компьютера в определенном подразделении. С помощью поддержки режима замыкания групповой политики можно определить два варианта получения списка объектов групповой политики для любого пользователя компьютеров в определенном подразделении:

* Режим слияния  
  В этом режиме при входе пользователя в систему список объектов групповой политики пользователя, как правило, объединяется при помощи функции GetGPOList. После этого функция GetGPOList вызывается снова с использованием расположения компьютера в службе Active Directory. После этого список объектов групповой политики добавляется в конец списка объектов групповой политики пользователя. Это происходит потому, что объекты групповой политики компьютера имеют более высокий приоритет, чем объекты групповой политики пользователя. В этом примере список объектов групповой политики компьютера был добавлен в список пользователя.
* Режим замещения  
  В этом режиме списки объектов групповой политики не объединяются. Используется только список объектов групповой политики, основанный на объекте компьютера.

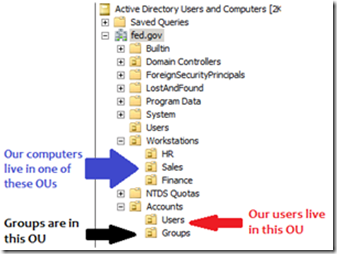
## [Групповая политика: замыкание на себя](http://system-administrators.info/?p=4452)

В данной статье я хотел бы рассказать о такой замечательной опции групповых политик, как loopback processing – замыкание на себя. Иногда сталкиваюсь с тем, что администраторы просто не знают про такую возможность и усложняют организационную структуру AD. Проще всего описать поведение данной политики на живом примере.

Итак, предположим в глобальной групповой политике **Default Domain Policy** определен таймаут скринсейвера в 30 минут. Данная политика настроена в разделеUser Configuration.



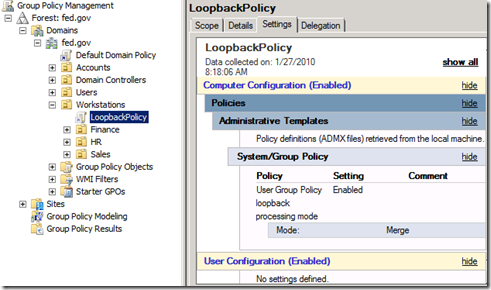
Теперь посмотрим где расположены объекты, с которым мы будем эксперементировать:



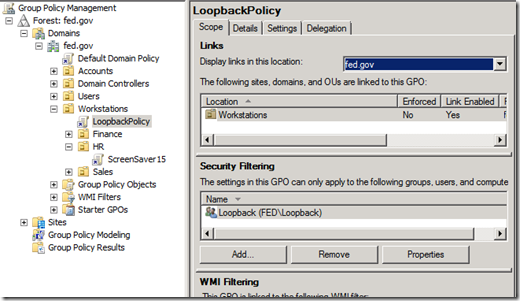
Хотя в целом подобная настройка скринсейвера подходит в большинстве случаев, может возникнуть ситуация когда для определенных компьютеров нужно изменить поведение скринсейвера. Предположим что для компьютеров, расположенных в OU HR нам необходимо изменить поведение скринсейвера, а для двух других OU оставить поведение групповой политики по умолчанию.

Для выполнения данной задачи мы используем режим замыкания политики на себя для принудительного применения настроек пользователя в групповой политике, применяемой к организационной единице, содержащей рабочие станции. Так как все остальные пользовательские политики должны применяться в полном объеме, мы будем использовать замыкание на себя с объединением.

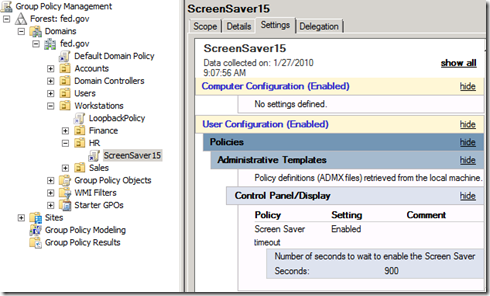
Создадим новую групповую политику, прикрепленную к **Workstations** OU.



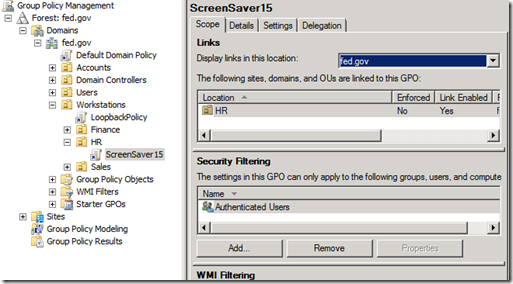
Так как в данном случае эта политика примениться ко всем дочерним разделам, нам необходимо контролировать к каким рабочим станциям будет применяться наша политика. Для этого создадим новую группу безопасности **Loopback** и разделе Security Filtering удалим права Read и Apply у группы **Authenticated Users.**После чего дадим эти права на свежесозданную группу **Loopback**.



Мы знаем что опция для настройки скринсейвера настраивается в разделе User Configuration групповой политики и обычно применяется на пользователей. Однако, так как мы используем замыкание на себя, мы настроим нужное нам значение скринсейвера в разделе User Configuration новой политики **ScreenSaver15**и прилинкуем данную политику на OU, где расположены рабочие станции.

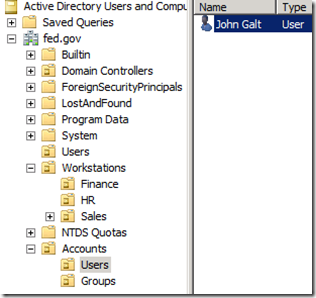


Так как политика замыкания на себя фильтруется на более верхнем уровне, в политике **ScreenSaver15** мы оставляем права Read и Apply по умолчанию.

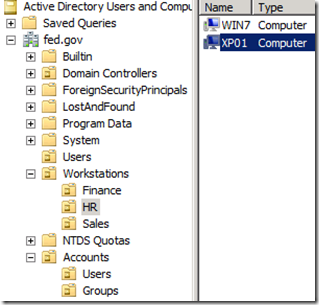


Итак, настройка закончена и теперь нам необходимо приступить к проверке того факта, что для любого пользователя, залогинившегося на компьютер, находящийся в OU HR, эффективный таймаут скринсейвера будет 15 минут вместо 30-ти.

Аккаунт пользователя, под которым мы будем выполнять проверку находиться в**Users** OU. Он называется **John.Galt**.



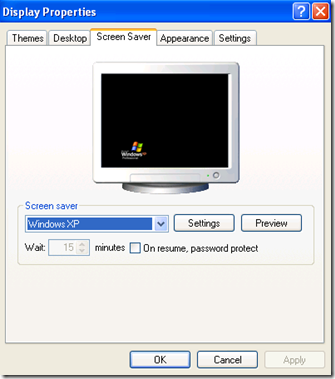
Аккаунт компьютера находиться в **HR**OU и называется **XP01**.



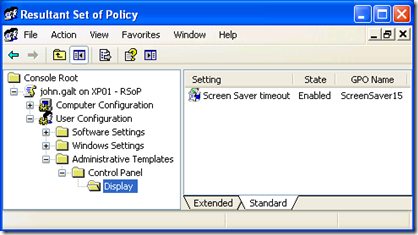
И данная рабочая станция добавлена в группу **Loopback**.



Теперь залогинимся под указанным пользователем на данный компьютер и посмотрим на параметры скринсейвера.



Запустив результирующую политику на этой машине мы увидим что применяется именно политика **ScreenSaver15** хотя OU HR содержит только объекты-компьютеры, а политика настроена в конфигурации пользователя..



Надеюсь в результате прочтения данной статьи вам удалось понять действие режима замыкания на себя. Хотелось бы отметить, что в некоторых сценариях возможно применение данной политики в режиме замены, при котором не происходит слияния. Конкретно для нашего примера это означало бы, что к любому пользователю после логона на компьютер **XP01** применилась бы только политика **ScreenSaver15**, все остальные политики были бы отброшены.