GiS ГАЗИНФОРМСЕРВИС

# Групповое управление параметрами безопасности в СЗИ от НСД «Блокхост-Сеть 2.0»

Сведения, описанные в данной статье, применимы начиная со сборки 2.2.16.1038 СЗИ от НСД «Блокхост-Сеть 2.0»

## 1. Общие сведения о групповом управлении параметрами безопасности

Начиная со сборки 2.2.16.1038 в серверной консоли «Блокхост-Сеть 2.0» (далее БХС) появились механизмы, позволяющие производить групповую настройку любых параметров безопасности СЗИ. Все механизмы безопасности в БХС можно разделить на две группы: настройки параметров безопасности рабочей станции и настройки безопасности пользователей рабочей станции. Настройки рабочей станции, также называемые **настройки машины**, применяются ко всем пользователям рабочей станции. **Настройки пользователей** - только к конечному пользователю или группе пользователей, для которых такая настройка выполнена. Групповая настройка параметров безопасности машин и параметров пользователей реализована в БХС двумя различными способами.

Для групповой настройки параметров обоих типов необходимо использовать **группы машин** в серверной консоли БХС. По умолчанию на сервере БХС уже имеется группа «Все машины», используемая как группа по умолчанию. Для более тонкой настройки вы можете создать нужные группы самостоятельно, при необходимости сгруппировав их в иерархию, соответствующую организации вашего предприятия. Также группы станций можно импортировать из хранилища Active Directory.

После добавления для каждой группы появится меню настройки параметров безопасности БХС, аналогичное меню настройки машины. По умолчанию это меню находиться справа от списка машин. Именно в нем и производится групповая настройка параметров безопасности. Параметры безопасности, настроенные в группе, распространяются на все машины в группе, а также на все вложенные группы и их станции. Таким образом, настраивая параметры верхней группы в иерархии, можно определять политику безопасности для всех вложенных групп и станций.

На уровне группы можно управлять настройками машин, добавлять группы пользователей и отдельные учетные записи. Для каждого типа таких объектов существуют свои особенности применения и механизмы использования.

## 2. Групповые настройки машин

К **настройкам машин** относятся следующие параметры: мандатный механизм, контроль целостности, очистка памяти, политики аутентификации, включение или отключение мягкого режима, адрес и порт syslog-сервера. Будучи определены на уровне группы, настройки перезаписывают любые значения аналогичных настроек на всех станциях и группах, находящихся ниже по иерархии. Настройки распространяются однократно при нажатии кнопки «синхронизировать» по всем группам и станциям иерархии. Определенные в верхней группе настройки действуют для всей иерархии, но могут быть переопределены на уровне нижних групп иерархии. Настройки будут применятся ко всем пользователям станций иерархии, независимо от других политик безопасности БХС. Для всей иерархии серверов и групп существует только одна политика для каждого параметра безопасности, которая может быть переопределена на нижних уровнях иерархии.

### 3. Групповые настройки пользователей

К **настройкам пользователей** относятся следующие механизмы безопасности БХС: временные папки, монопольный доступ, дискреционный механизм (включая гарантированное удаление), контроль портов, ограничения по времени, контроль процессов, контроль печати, персональный экран, полномочия администратора, аутентификация. Для каждого механизма или для группы механизмов может быть определенно неограниченное количество вариантов настройки. Каждый такой вариант должен быть привязан к существующей доменной группе пользователей. **Группа пользователей Active Directory с привязанным к ним настройками пользовательских механизмов БХС получила название – политика групп пользователей** (здесь и далее ПГП). Созданные политики групп пользователей постоянно распространяются по иерархии серверов и групп. О правилах применения ПГП на конечных рабочих станциях группах и механизмах определения результирующих настроек для конечного пользователя, входящего в несколько или одну группу пользователей можно прочитать в пункте «управление политиками групп пользователей» данного руководства. В иерархии может существовать неограниченно количество ПГП, которые могут быть определенны на любых уровнях иерархии. ПГП, определенная на уровне отдельной станции БХС, не распространяется по иерархии и действует только на станции, где она была создана. Во всех случаях настройки ПГП (если они определены) приоритетнее настроек пользователя, заведенного в консоли напрямую

### 4. Групповое добавление пользователей

Также на уровне группы станций БХС могут быть добавлены пользователи домена. При синхронизации такие пользователи будут внесены в списки пользователей станций, находящихся внутри группы с теми настройками, которые были определены на уровне группы. Если аналогичные пользователи уже есть на станциях, где проходит синхронизация, то их настройки будут перезаписаны в соответствии с настройками пользователя на уровне группы. Добавленный таким методом пользователь не будет пользоваться приоритетом групповых политик, значение его пользовательских настроек могут быть изменены любой ПГП, действующей на конечной станции. Добавление пользователя на станции в иерархии группы выполняется однократно по нажатию кнопки синхронизации в меню управления группой, дальнейшей автоматической синхронизации не происходит.

### 5. Режимы работы ПГП и групповых настроек параметров машин.

При первичной установке сервера БХС все групповые настройки БХС находятся в состоянии **«не задано»**. В интерфейсе серверной консоли такое состояние отображается как перечёркнутое название пользовательского механизма или настройки. В этом состоянии групповые настройки считаются выставленными в значение по умолчанию и не распространяются вниз по иерархии серверов.

Администратор безопасности с помощью контекстного меню управления настройками группы может выполнить действие «задать настройки». Задание списка пользователей позволяет создавать ПГП или добавлять пользователей для распространения вниз на подчиненные сервера или по иерархии групп. При добавлении ПГП в заданный список

пользователей все ее механизмы являются «не заданными» и учитываться на нижних уровнях не будут. Для того, чтобы ПГП установила какие-либо параметры для пользователей, каждый механизм необходимо «задать». После этого он перестанет отображаться в интерфейсе серверной консоли как зачеркнутый и станет учитываться на нижних уровнях иерархии при выборе результирующих политик для пользователей, которые входят в доменную группу, на основе которой была создана данная ПГП.

Любые «заданные» настройки можно переопределить на любом нижнем уровне иерархии, так как они будут открыты для редактирования. В случае, если у группы или сервера, где было выполнено переопределение, есть свои дочерние группы или сервера, то на них будут распространяться уже переопределенные настройки.

Если администратор безопасности хочет распространить по иерархии какие-либо настройки без возможности их переопределения на уровнях ниже, то следует использовать так называемый **режим «замок»**. Режим «замок» означает, что настройка или ПГП не может переопределена на нижних уровнях иерархии, по которой она распространяется.

## 5. Управление политиками групп пользователей

Как уже говорилось, количество ПГП для группы машин или станции неограниченно. Так как ПГП основаны на доменных группах безопасности, то один и тот же пользователь может входить в несколько групп пользователей, и на него будет распространятся действия нескольких ПГП. Кроме того, в различных ПГП для пользователя могут быть определены различные механизмы безопасности, причем в каждой ПГП такой набор механизмов будет уникальным.

Для понимания механизма определения настроек конечного пользователя в этом случае рассмотрим конкретный пример. Допустим, пользователь входит в следующие доменные группы: группа 1, группа 2 и группа 3. На основе этих групп созданы одноименные ПГП, механизмы в них определены согласно таблице 1. Значение от set1 до set 9 – уникальные настройки механизмов ПГП, заданные администратором безопасности.

Таблица 1: Настройки ПГП

| Наименование ПГП | Приоритет | Дискр. механизм | Контроль портов | Контроль печати | Контроль процессов | Аутентификация |
|---|---|---|---|---|---|---|
| Группа 1 | 1 | Set1 | Не задано | Set2 | Set3 | Не задано |
| Группа 2 | 2 | Не задано | Set4 | Не задано | Set5 | Не задано |
| Группа 3 | 3 | Set6 | Set7 | Set8 | Не задано | Set9 |

Если пользователь входит во все три группы одновременно, то заданные настройки (у нас они обозначены термином set) буду браться из группы, обладающей наибольшим приоритетом. В БХС 2.2 приоритет – это число, сопоставленное каждой ПГП. Чем меньше это число, тем выше приоритет. Таким образом, максимальным приоритетом в нашей таблице обладает группа 1 с приоритетом 1, минимальным приоритетом: группа 3 с приоритетом 3. Если же настройки в самой приоритетной группе не заданы, то берутся заданные настройки из ПГП со следующим по значению приоритетом. Если настройки

механизма не заданы ни в одной из ПГП, то пользователь получает дефолтные настройки, или те настройки, которые были заданы ему вручную. Таким образом, пользователь, входящий во все три ПГП, получит следующий набор настроек:

Таблица 2: Результирующие настройки пользователя

| Дискр. Механизм | Контроль портов | Контроль печати | Контроль процессов | Аутентификация |
|---|---|---|---|---|
| Set1 | Set4 | Set2 | Set3 | Set9 |

Дискреционный механизм, контроль печати и контроль процессов заданы в группе 1, которая является наиболее приоритетной (значение приоритета 1), поэтому пользователь получит настройки этих механизмов из группы 1. Контроль портов пользователь получит из группы 2, так как в группе 1 механизм не задан, а значение приоритета группы 2 меньше, чем группы 3. Значение аутентификации пользователь получит из группы 3, хотя она и наименее приоритетная из всех, так как в других группах этот параметр не задан.

Приоритет ПГП может быть изменен администраторам безопасности вручную на любом уровне иерархии с помощью окна управления приоритетом. Чтобы избежать этого, администратор может использовать режим замок на приоритете любой ПГП. Приоритет такой ПГП будет нельзя поменять на нижних уровнях иерархи. С помощью постановки «замка» на приоритете администратор безопасности может создать ПГП для группы пользователей, которая будет главной на нижних уровнях иерархии, любые члены данной группы будут получать настройки из этой ПГП.

Режим «замок» также можно распространить на любой отдельный механизм безопасности внутри ПГП. На практике это означает, что администратор не сможет переопределить этот механизм на нижних уровнях иерархии в данной ПГП.

Также «замком» можно зафиксировать список пользователей и приоритет ПГП (см. управление политиками групп пользователей). Если список пользователей распространен в режиме «замок», то все станции и группы снизу по иерархии будут использовать список пользователей тождественный тому, который был задан на верхней группе иерархии. Все добавленные ПГП и пользователи на нижних уровнях иерархии будут удалены, вместо них будет записано содержимое списка пользователей, распространяемое в режиме «замок» с главной группы иерархии. Следует с большой осторожностью пользоваться возможностью установки режима «замок» на список пользователей, так как это может привезти к невозможности входа пользователей на станции и другим отказам, связанным с изменением настроек станций БХС. Основные отказы в этом случае будут связаны с удалением из списка пользователей алиаса «Гость». Как известно, этот алиас указывает политику обработки учетных записей, не указанных в консоли клиента БХС напрямую. Его удаление приводит к невозможности работы таких учетных записей на станции, что в свою очередь может привести к отказу в работе приложений и служб, и даже к отказу в доступе к станции. При использовании списка пользователей в режиме замок настойчиво рекомендуем вручную добавлять на станции алиас «Гость» обратно! Сделать это можно, добавив в консоли локального пользователя «Гость» на клиентах БХС.

# Практические примеры использования группового управления параметрами безопасности БХС

Рассмотрим практические примеры использования механизмов групповой настройки БХС для вымышленной компании Contoso. В этой компании развернут сервер БХС и несколько подключенных к нему клиентов, объединенных в иерархию как на рисунке 1.

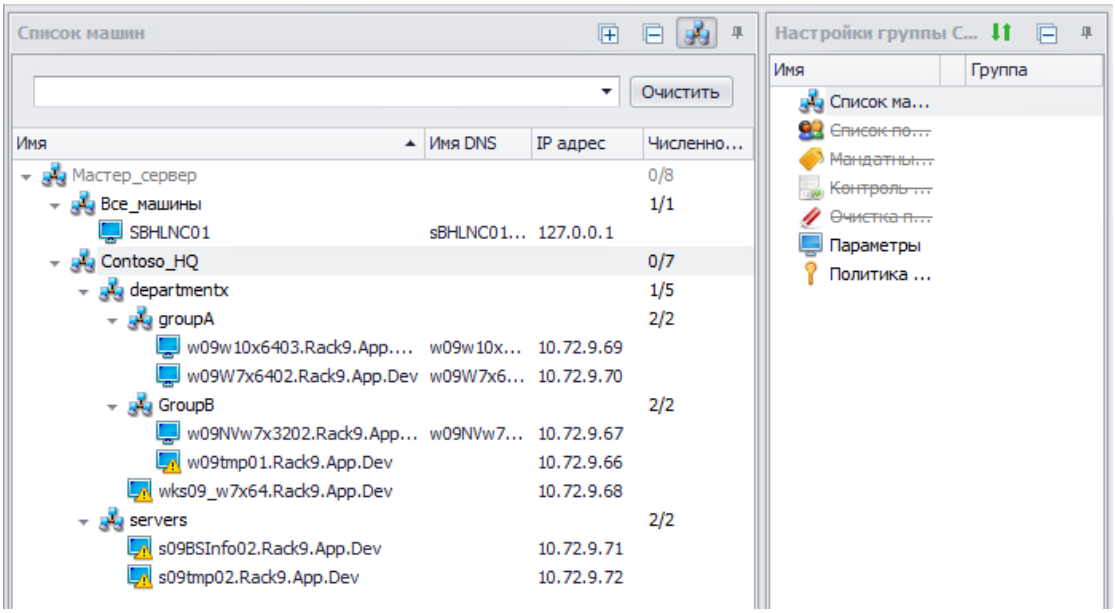



Рисунок 1: Иерархия Contoso

В предприятии работает некоторое количество сотрудников, для которых созданы учетные записи пользователей, сами учетные записи объединены в группы безопасности в домене RACK9. В организации работают следующие вымышленные пользователи**: Andrew Ivanov, James Sidorov, Sergei Petrov, Piter Rogachev, AdminAdminov и Great manager**. Они включены в группы **безопасности contoso_user, department_admin и head_stuff** согласно таблице ниже:

| Группа | contoso_user | department_admin | head_stuff |
|---|---|---|---|
| Включенные пользователи | Andrew Ivanov<br>James Sidorov<br>Sergei Petrov<br>Piter Rogachev<br>AdminAdminov<br>Great manager | AdminAdminov | Great manager |

Исходные данные, приведенные выше, будут одинаковыми для всех описываемых примеров.

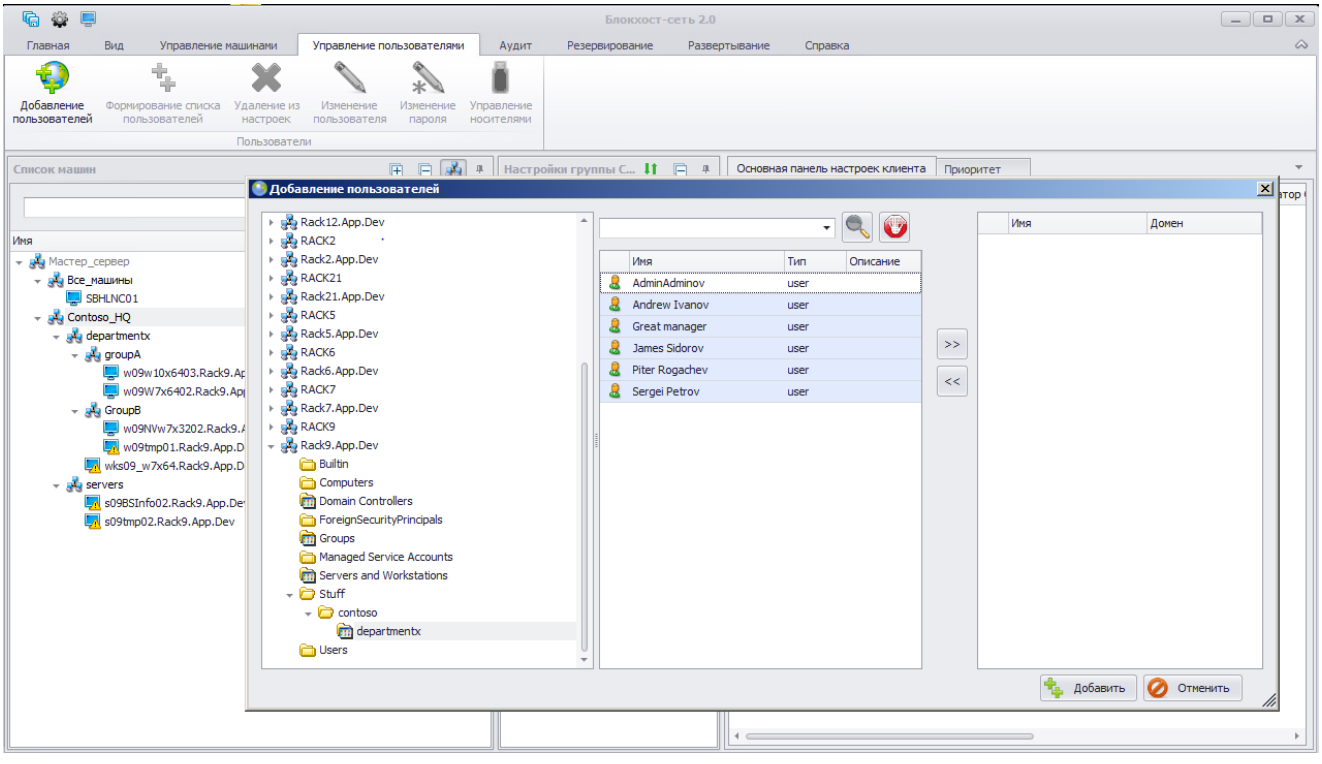
## Пример 1: Настройка принудительной двухфакторной аутентификации (вход по токену) для пользователей Contoso

Задача: необходимо настроить принудительную двухфакторную аутентификацию для членов группы contoso_user, при этом пользователь AdminAdminov должен аутентифицироваться на всех машинах компании без токена.

Для начала реализации этой задачи нужно понимать, что в архитектуре БХС вход по токену технически возможен только тогда, когда пользователь добавлен на конечную машину в консоли БХС и ему присвоен токен, с которым будет осуществляться аутентификация. Если нам известно на каких конечных машинах работают пользователи Contoso, то необходимо добавить пользователя с токеном на каждую такую машину, для обеспечения технической возможности входа по токену.

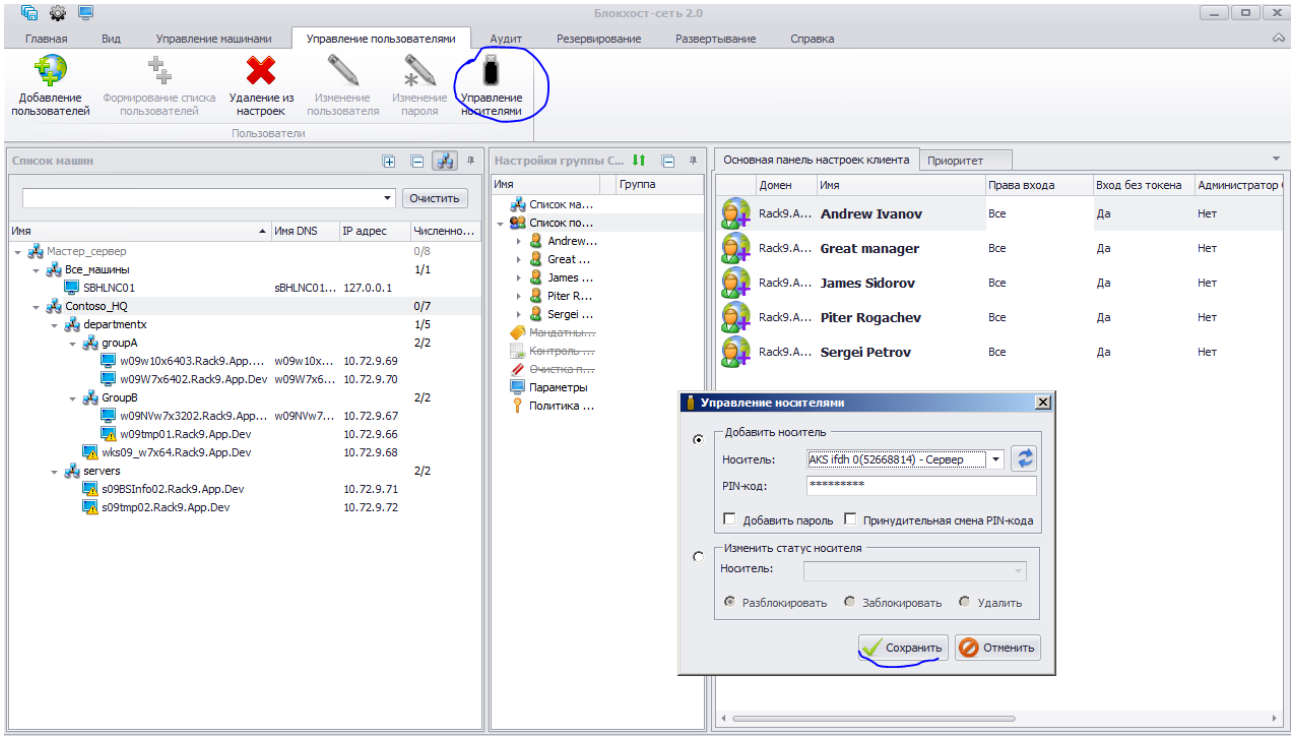
Если же нам неизвестно, на какой машине работает тот или иной пользователь, или необходимо обеспечить работу всех пользователей на всех станциях в режиме двухфакторной аутентификации, то необходимо будет воспользоваться функционалом группового добавления пользователей.

Для этого в списке машин сервера БХС необходимо выбрать группу Contoso_HQ. В настройках группы задать список пользователей. Далее, добавить в список пользователей Andrew Ivanov, James Sidorov, Sergei Petrov, Piter Rogachevи Great manager. Пользователя AdminAdminov добавлять не будем, так как по условиям задачи он должен входить без токена.



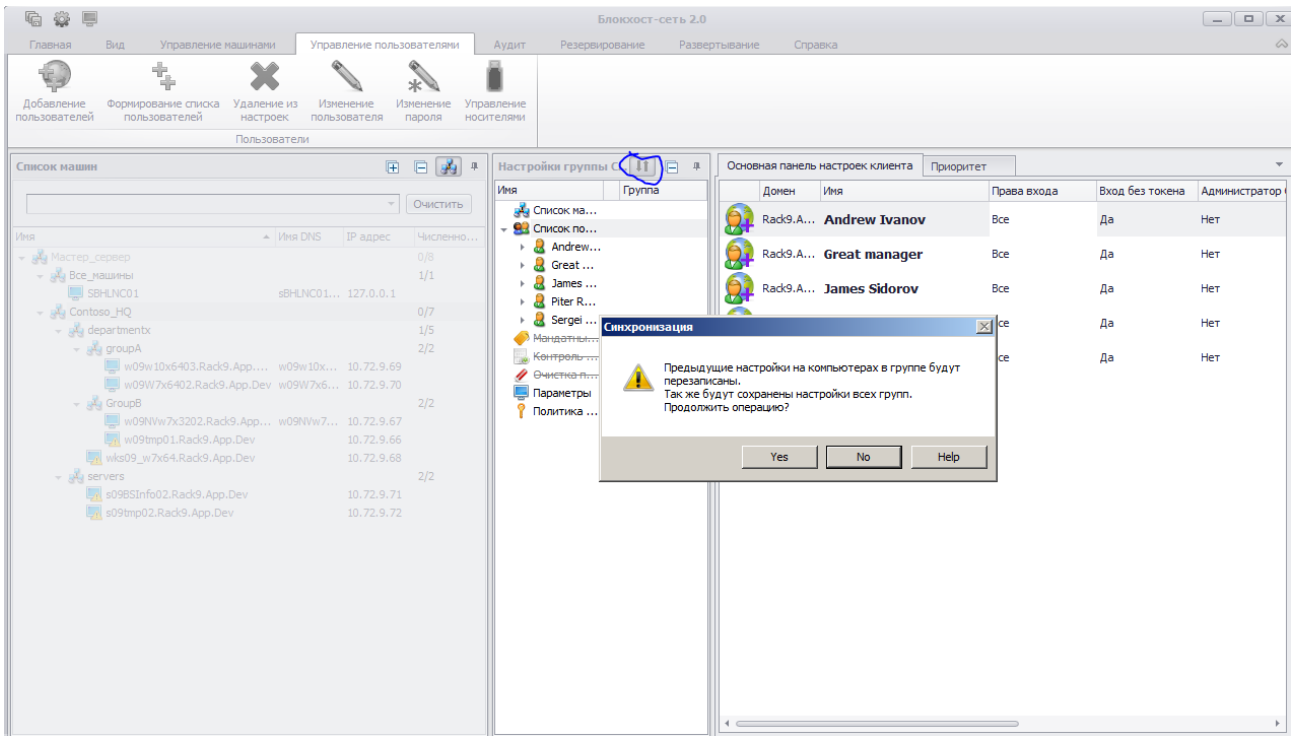
Добавление пользователей в группу Contoso HQ

Далее добавляем каждому пользователю токен. В нашем случае токен подключен к серверу.




Добавление токена пользователю Andrew Ivanov

Когда токены всех пользователей будут добавлены, нужно произвести групповую синхронизацию настроек



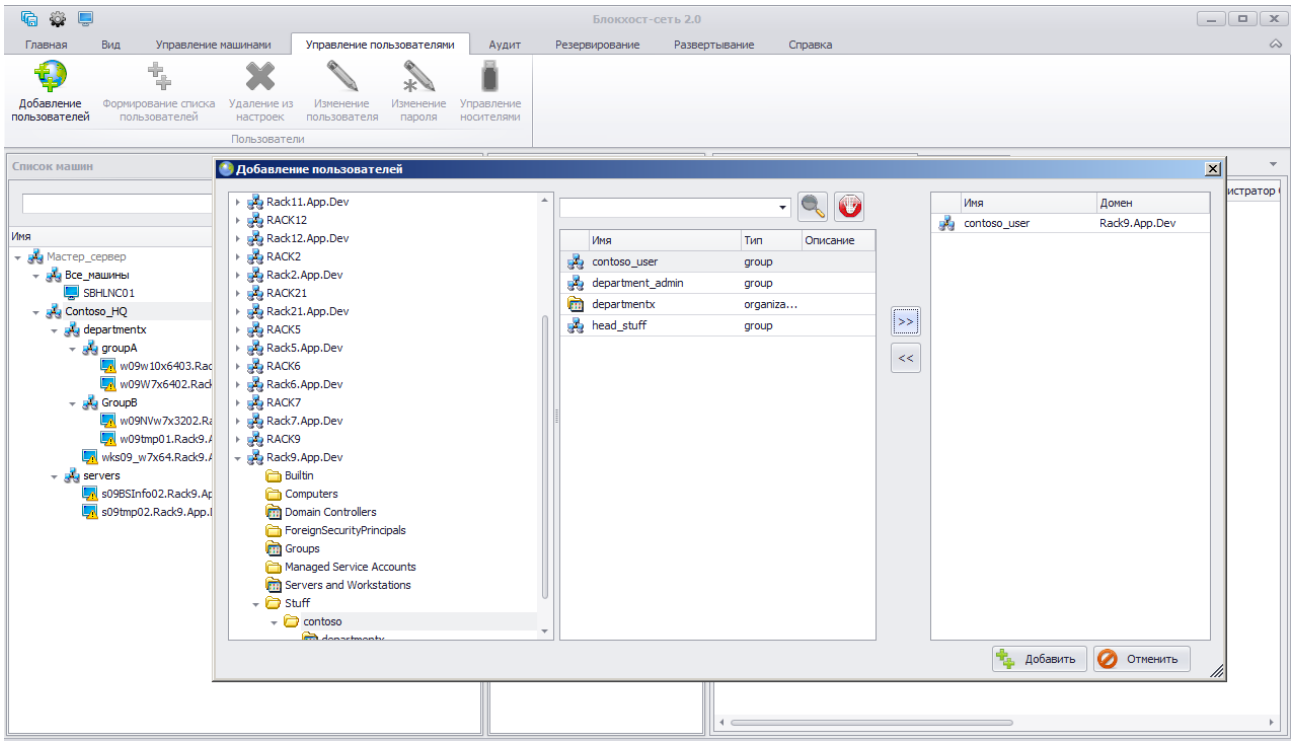

Групповая синхронизация

После синхронизации наш список пользователей будет добавлен на все машины иерархии.

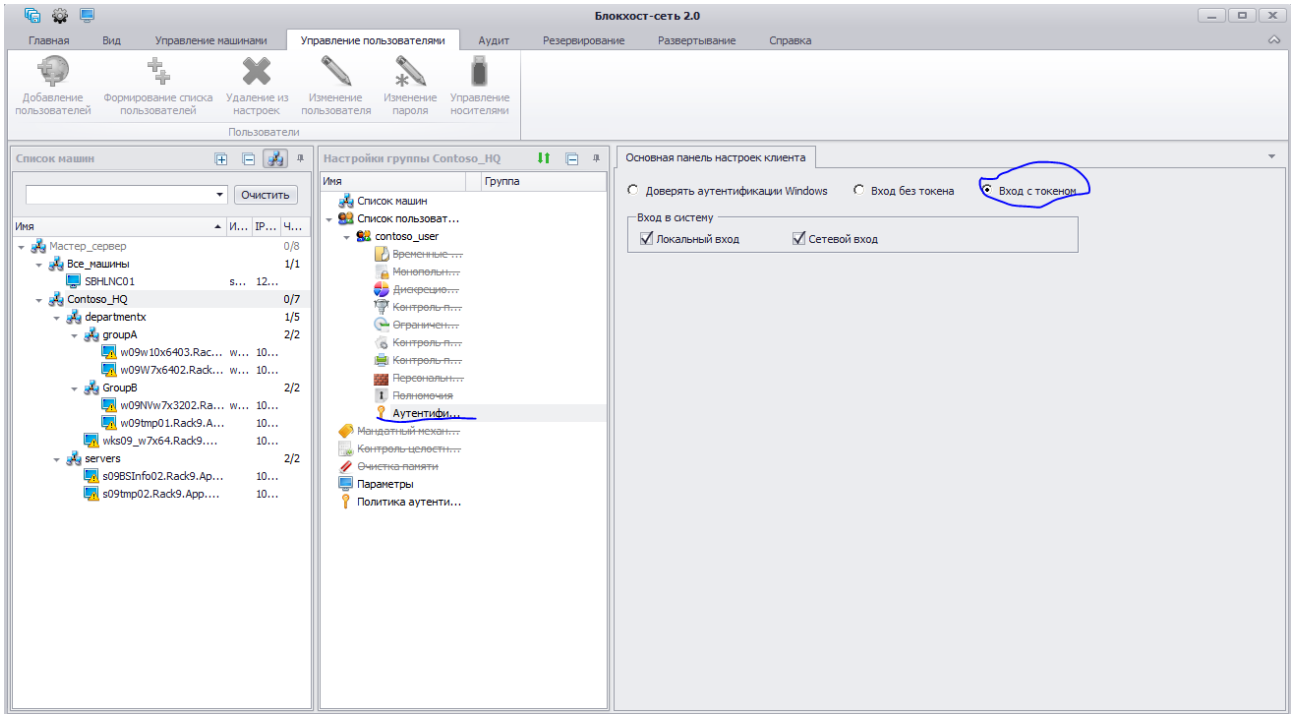
Далее необходимо очистить список пользователей группы Contoso HQ и приступить к созданию ПГП, обеспечивающий двухфакторную аутентификацию.

Добавляем ПГП для доменной группы contoso_user в группе машин Contoso HQ и настраиваем в ней для пользователей принудительный вход по токену.

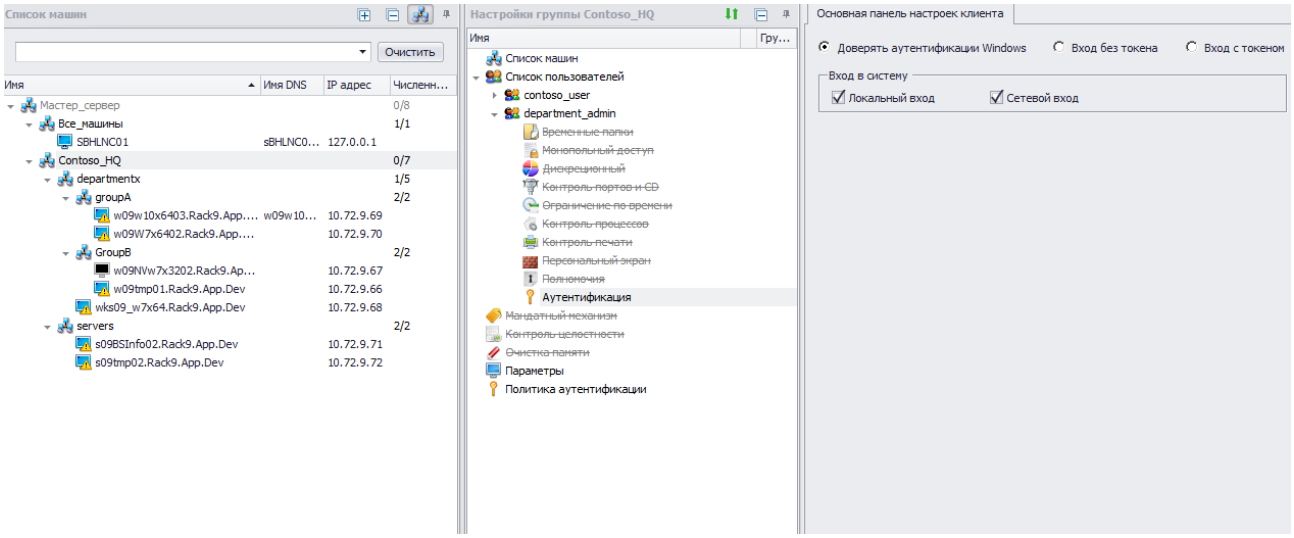
Добавляем и конфигурируем ПГП:




После создания политики задаем механизм «Аутентификация» и конфигурируем его для входа по токену.




Аналогичным образом создаем в Contoso HQ ПГП для доменной группы department_admin с другой политикой аутентификации: для нее будет задано значение “доверять аутентификации windows”

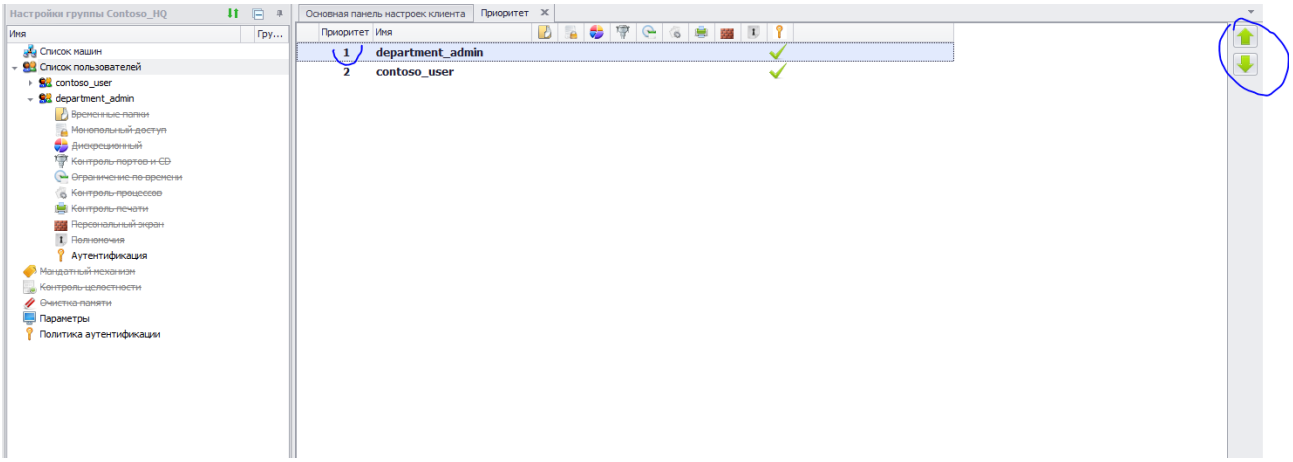



Создание ПГП department_admin с настройкой “доверять аутентификации windows”

Так как пользователь Admin Adminov, для которого необходимо задать исключение, входит в обе группы, то нам необходимо сконфигурировать приоритет ПГП department_admin так, чтобы ее настройки были главнее настройки ПГП contoso_user.

Для этого нам надо открыть окно «управление приоритетом». Сделать это надо на списке пользователей группы машины Contoso HQ. Мы видим, что ПГП contoso_user имеет приоритет 1, а ПГП department_admin – 2. Значит, на текущий момент настройки группы contoso_user более приоритетны, и пользователь Admin Adminov должен будет аутентифицироваться по токену. Чтобы изменить это, необходимо поменять порядок

приоритета наших ПГП. Сделать это можно с помощью зеленных стрелок справа в окне управления приоритетом




После регулирования приоритета для Admin Adminov будет обеспечен приоритет аутентификации без токена, что полностью удовлетворяет условию задачи. Теперь остается только провести синхронизацию настроек по иерархии Contoso HQ и задача будет выполнена.