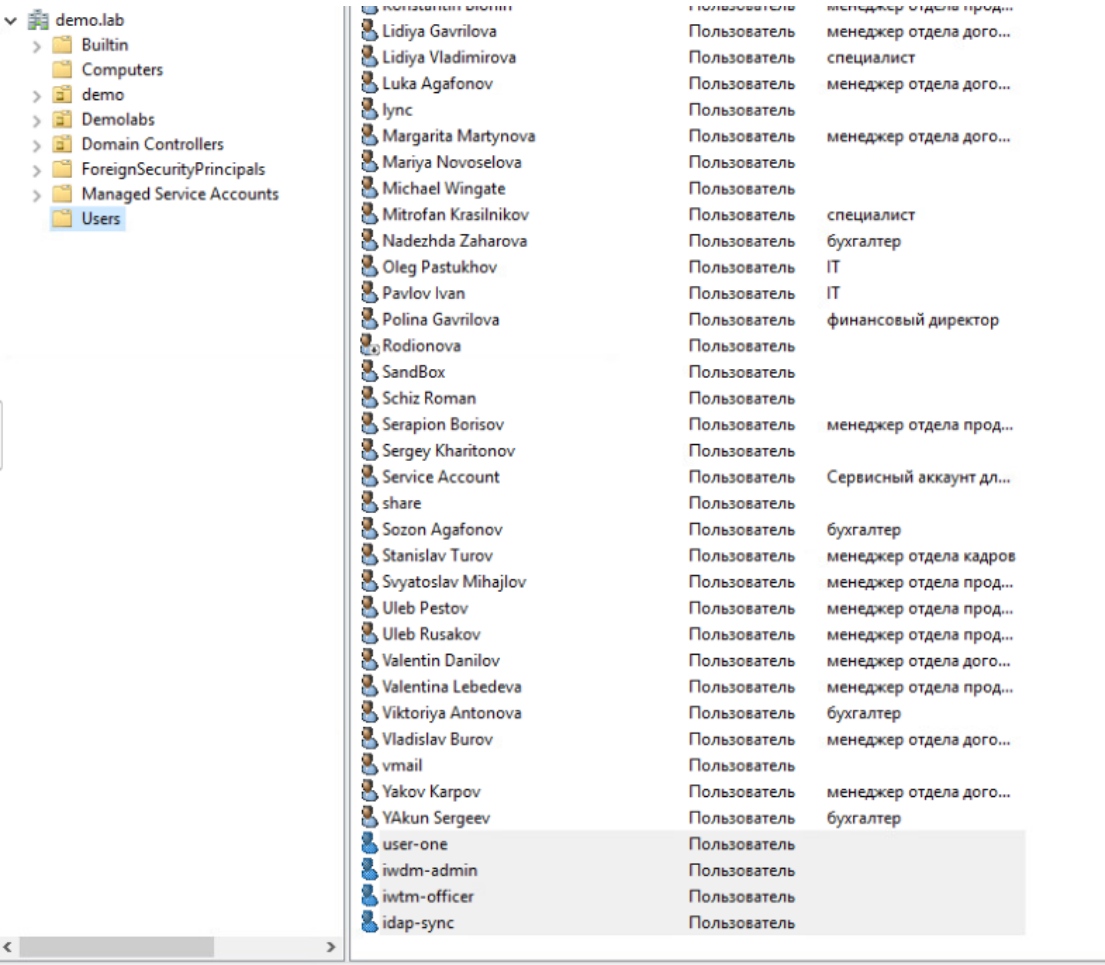


Задание 1: Настройка контроллера домена

В корневом каталоге оснастки «Пользователи и компьютеры» AD сервера необходимо создать и настроить следующих доменных пользователей с соответствующими правами:

- Логин: user-one, пароль: xxXX1234, права пользователя домена
- Логин: iwdm-admin, пароль: xxXX1234, права администратора домена
- Логин: iwtm-officer, пароль: xxXX1234, права пользователя домена
- Логин: ldap-sync, пароль: xxXX1234, права пользователя домена

Создали юзеров, делегировали их.



Задание 2: Настройка DLP сервера

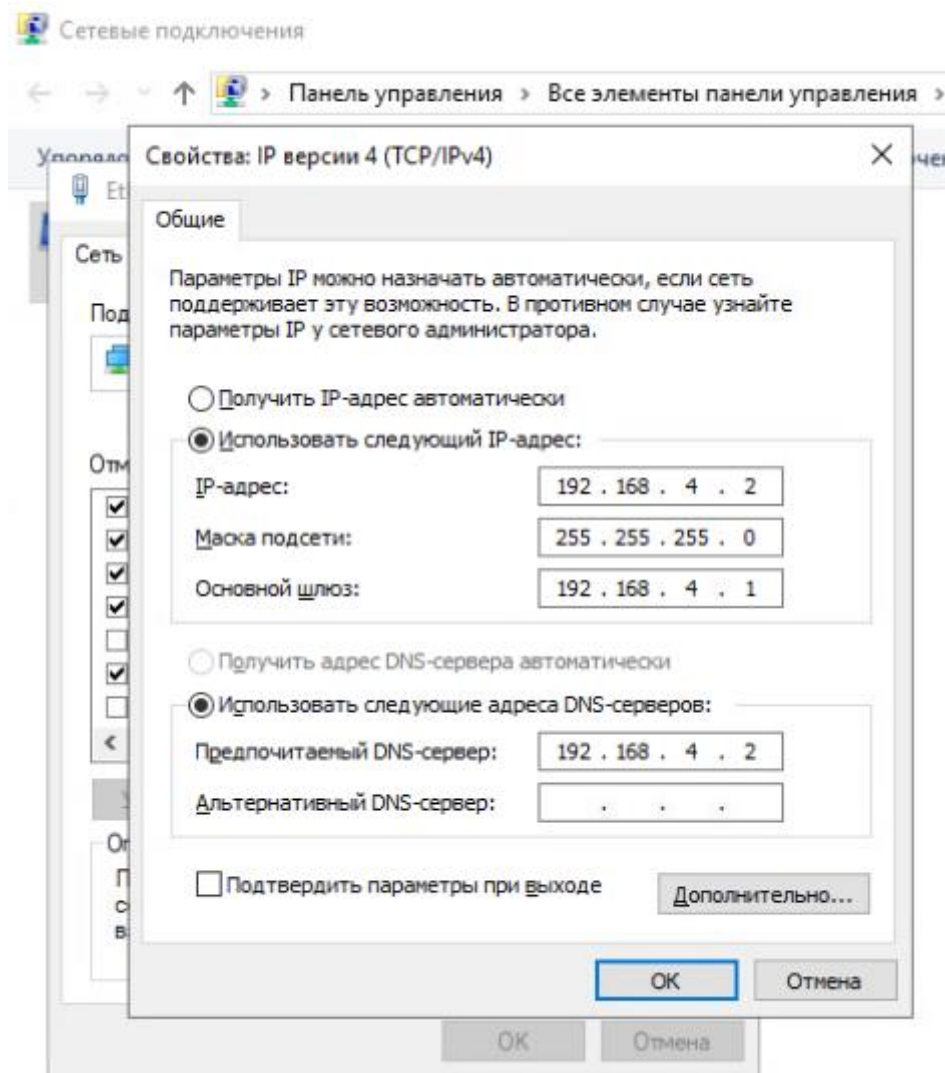
DLP-сервер контроля сетевого трафика уже предустановлен, но не настроен.

Необходимо синхронизировать каталог пользователей и компьютеров LDAP с домена с помощью ранее созданного пользователя ldap-sync.

Для входа в веб-консоль необходимо настроить использование ранее созданного пользователя домена iwtm-officer с полными правами офицера безопасности и на администрирование системы, полный доступ на все области видимости.

Запишите IP-адреса, токен, логины и пароли от учетных записей, а также все прочие нестандартные данные (измененные вами) вашей системы в текстовом файле «отчет.txt» на рабочем столе компьютера.

В demo.lab делаем:



Теперь запускаем центос:

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1160.el7.x86_64 on an x86_64

iwtm login: root
Password:
Last login: Wed Nov 17 09:08:09 on tty1
[root@iwtm ~]# nmtui_
```

Ставим категорию manual и пишем адреса:

Edit Connection

Profile nameens32

Deviceens32 (00:8C:29:97:F9:CA)

= ETHERNET

Show

IPv4 CONFIGURATIONManual

Hide

Addresses192.168.4.3/24

Remove

Add...

Gateway192.168.4.1

DNS servers192.168.4.2

Remove

Add...

Search domainsAdd...

Routing (No custom routes) Edit...

☐ Never use this network for default route

☐ Ignore automatically obtained routes

☐ Ignore automatically obtained DNS parameters

☒ Require IPv4 addressing for this connection

= IPv6 CONFIGURATIONAutomatic

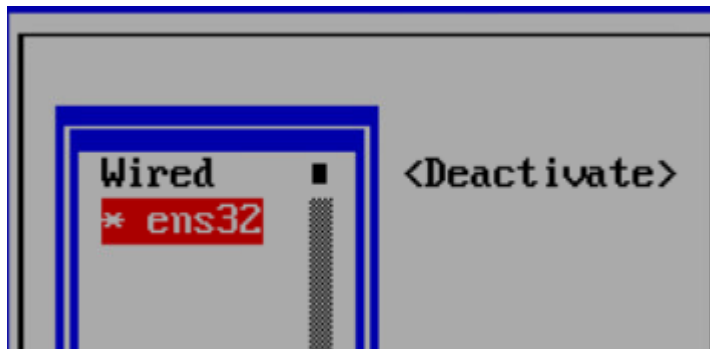
Show

☒ Automatically connect

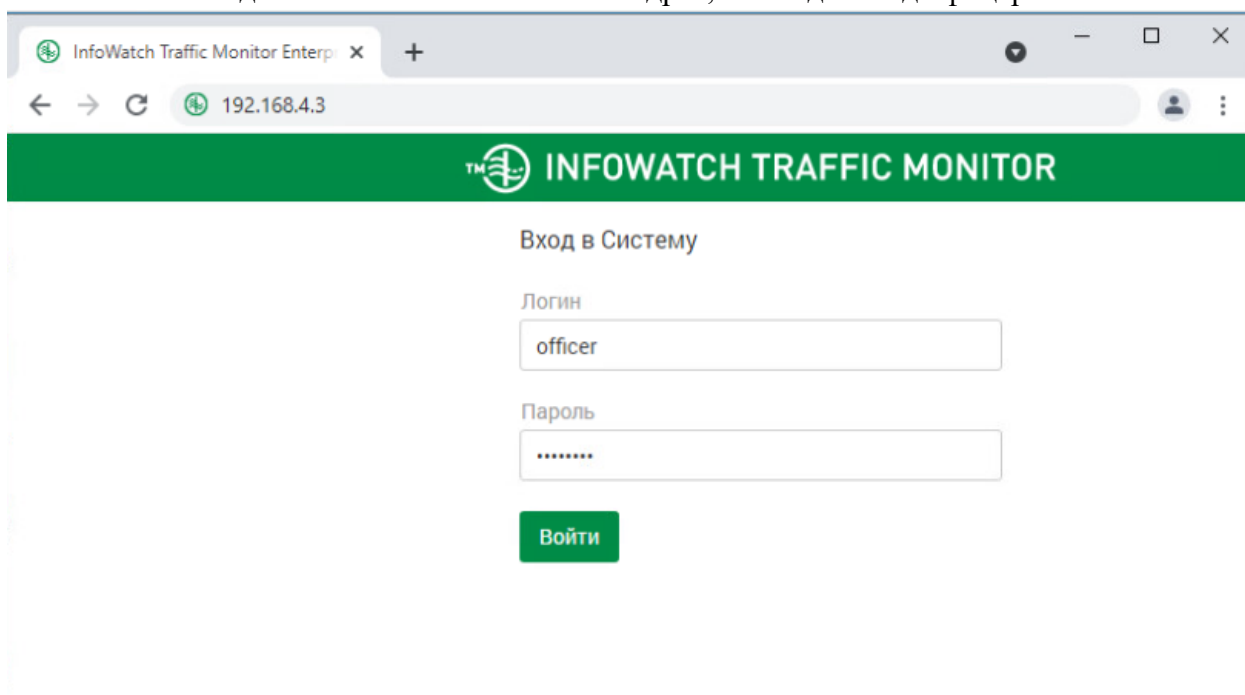
☒ Available to all users

CancelOK

Далее заходим в актив конект и ребутаем клавишей энтер:



После этого заходим в demo.lab и вписываем адрес, и заходим под офицером:



Заходим:

Управление ▾

Краулер

LDAP-синхронизация

И добавляем:

Добавление LDAP-сервера

Имя сервера

demo

Тип сервера

Active Directory ▾

Синхронизация

Автоматическая

Ручная

Период синхронизации

Ежеминутно ▾

Повторение

15

↑

↓

минут

Настройки соединения

LDAP-сервер

192.168.4.2

Использовать протокол Kerberos

☐

Глобальный LDAP-порт

3268

↑

↓

LDAP-порт

389

↑

↓

Использовать глобальный каталог

☒

LDAP-запрос

dc=demo, dc=lab

Анонимный доступ

☐

Логин

ldap-sync

Пароль

Сохранить

Проверить соединение

Отменить

Далее создаём пользователя. [\управление доступом\создать пользователя\](#) и здесь вписываем:

Создание пользователя

>

Логин

iwtm-officer

Статус

Активен

▼

Email

demo@mail.ru

Полное имя

iwtm-officer

Роли

Администратор X

Офицер безопасности X

X ▼

+

Области видимости

Полный доступ X

VIP X

X ▼

+

Описание

Описание

Пароль

.....

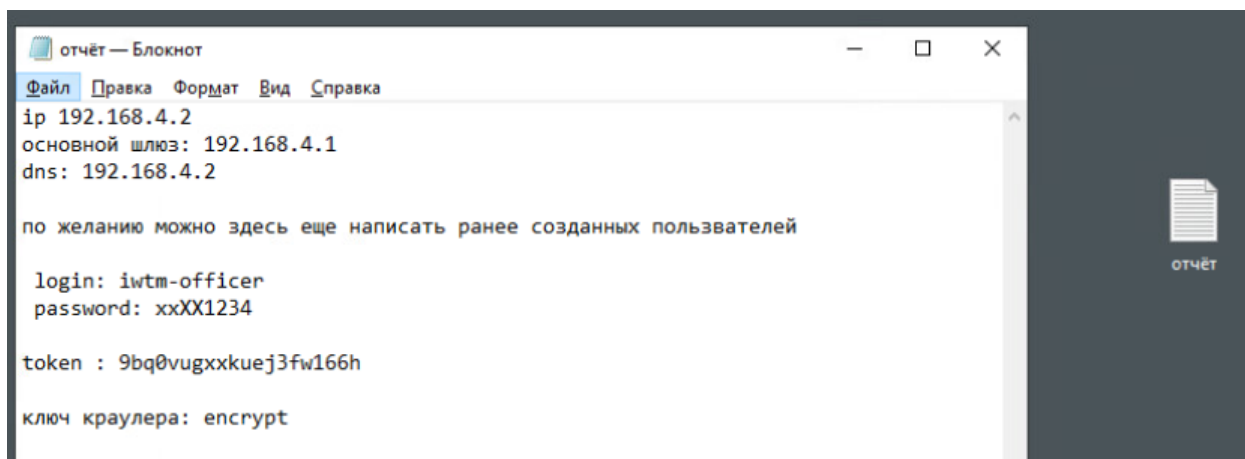
Подтверждение
пароля

.....

Сохранить

Отменить

Далее создаём отчёт в демо лабе



Задание 3: Установка и настройка сервера агентского мониторинга

Необходимо ввести сервер в домен, после перезагрузки войти в систему от ранее созданного пользователя `iwdm-admin` (важно). После входа в систему необходимо переместить введенный в домен компьютер.

Установить базу данных PostgreSQL с паролем суперпользователя `xxXX1234`.

Установить сервер агентского мониторинга с параметрами по умолчанию, подключившись к ранее созданной БД.

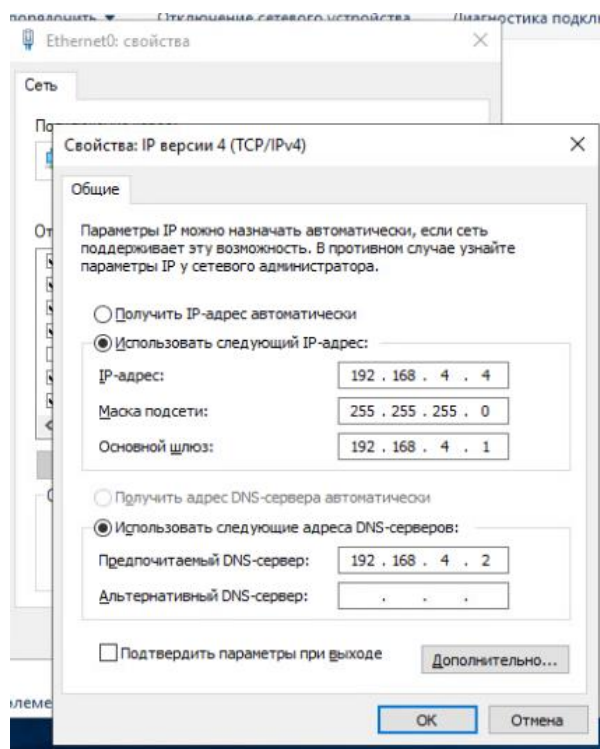
При установке сервера агентского мониторинга необходимо установить соединение с DLP-сервером по IP-адресу и токenu, но можно сделать это и после установки. При установке настроить локального пользователя консоли управления: `officer` с паролем `xxXX1234`

Синхронизировать каталог пользователей и компьютеров с Active Directory.

После синхронизации настроить беспарольный вход в консоль управления от ранее созданного доменного пользователя `iwdm-admin`, установить полный доступ к системе, установить все области видимости.

Проверить работоспособность входа в консоль управления без ввода пароля. Если сервер не введен в домен или работает от другого пользователя, данная опция работать не будет.

Заходим в `iwdm` и настраиваем инет



(по желанию) Проверили адрес, потерь нет, всё заебусик.

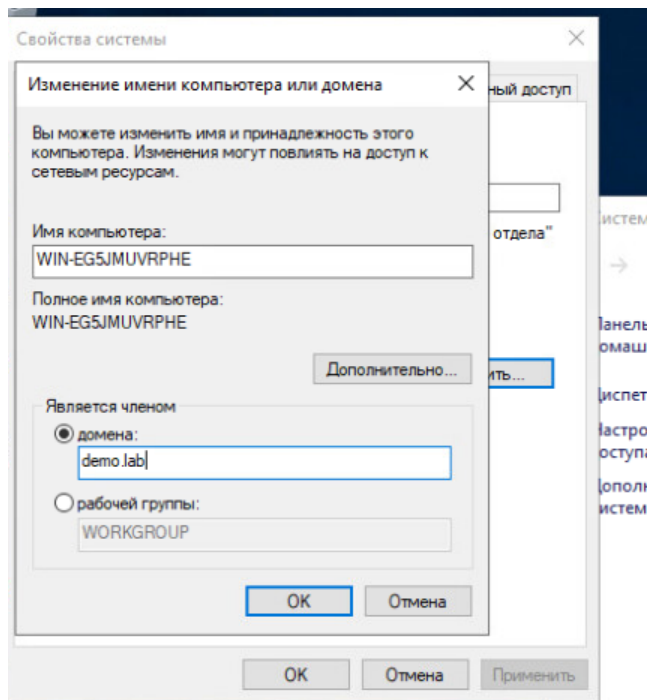
```
Администратор: Windows PowerShell
Windows PowerShell
(C) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

PS C:\Users\Администратор> ping 192.168.4.2

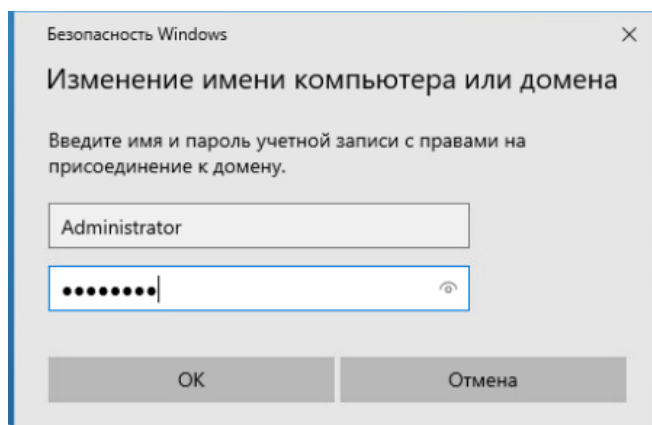
Обмен пакетами с 192.168.4.2 по с 32 байтами данных:
Ответ от 192.168.4.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.4.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.4.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.4.2: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.4.2:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
PS C:\Users\Администратор>
```

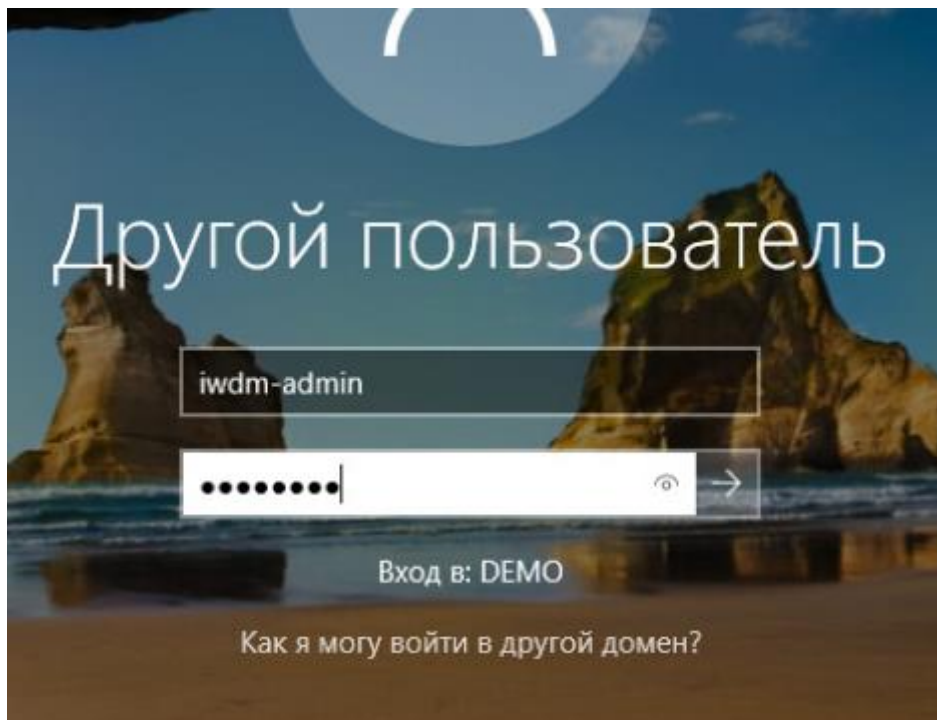
Далее вводим в домен эту машину:



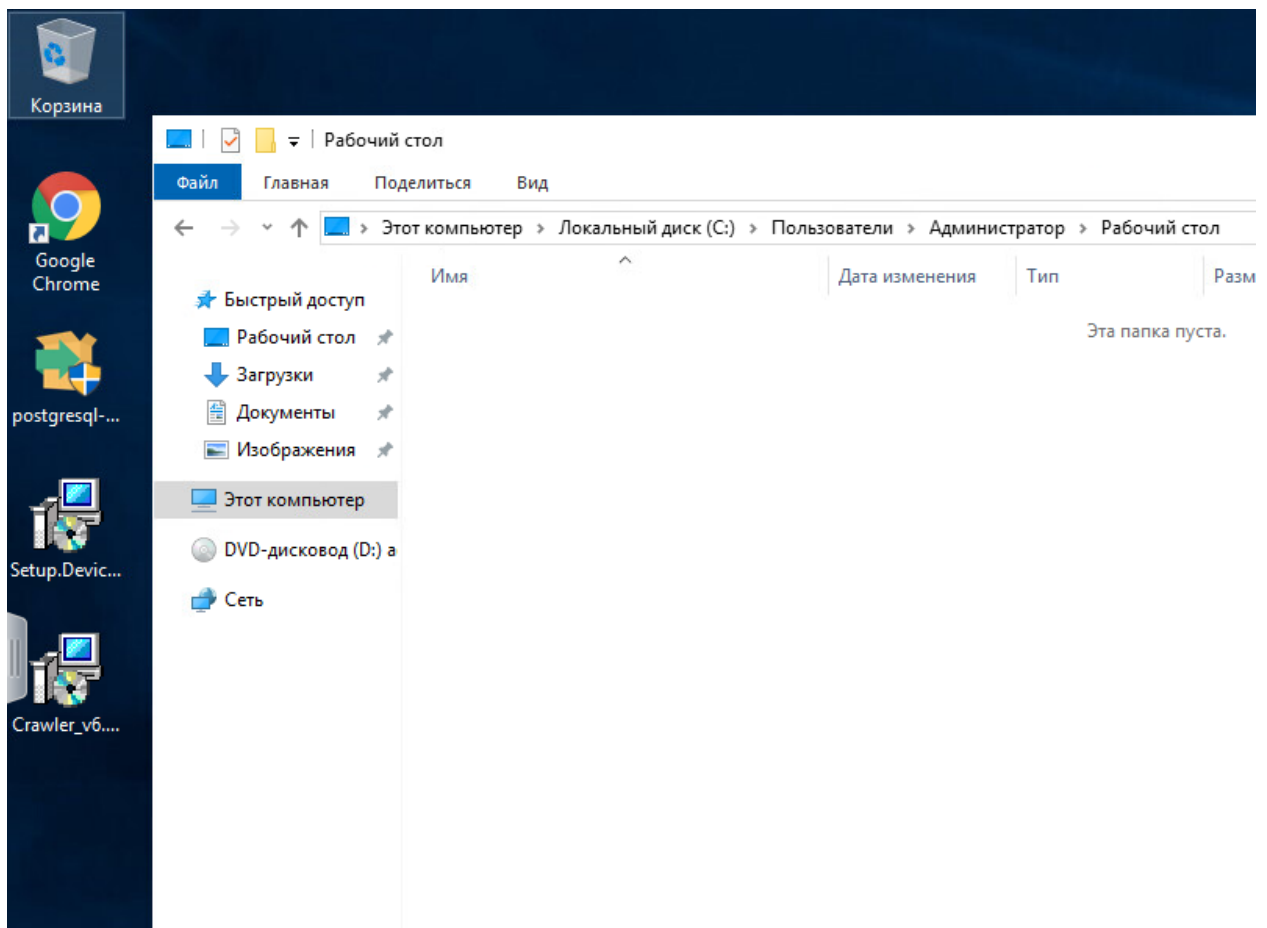
Вводим пароль



После ребута тачки заходим под таким логином:

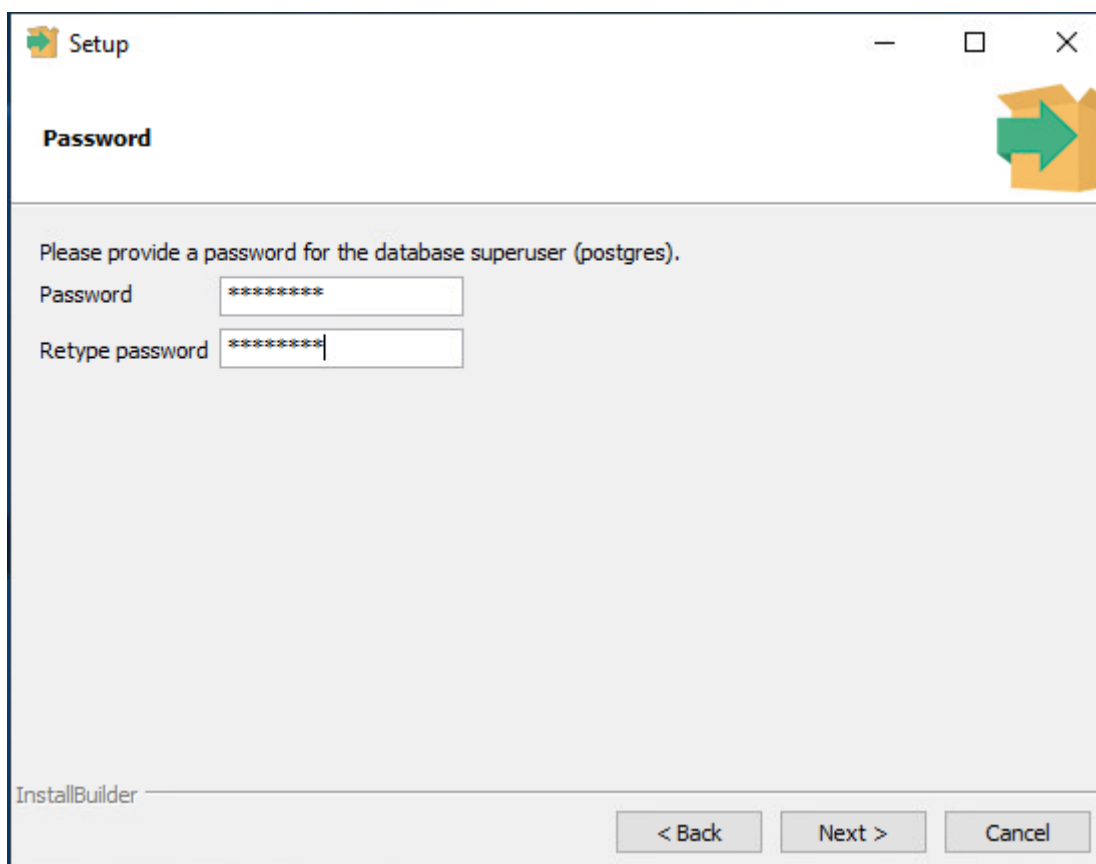


И перемещаем сетяпы на раб стол:



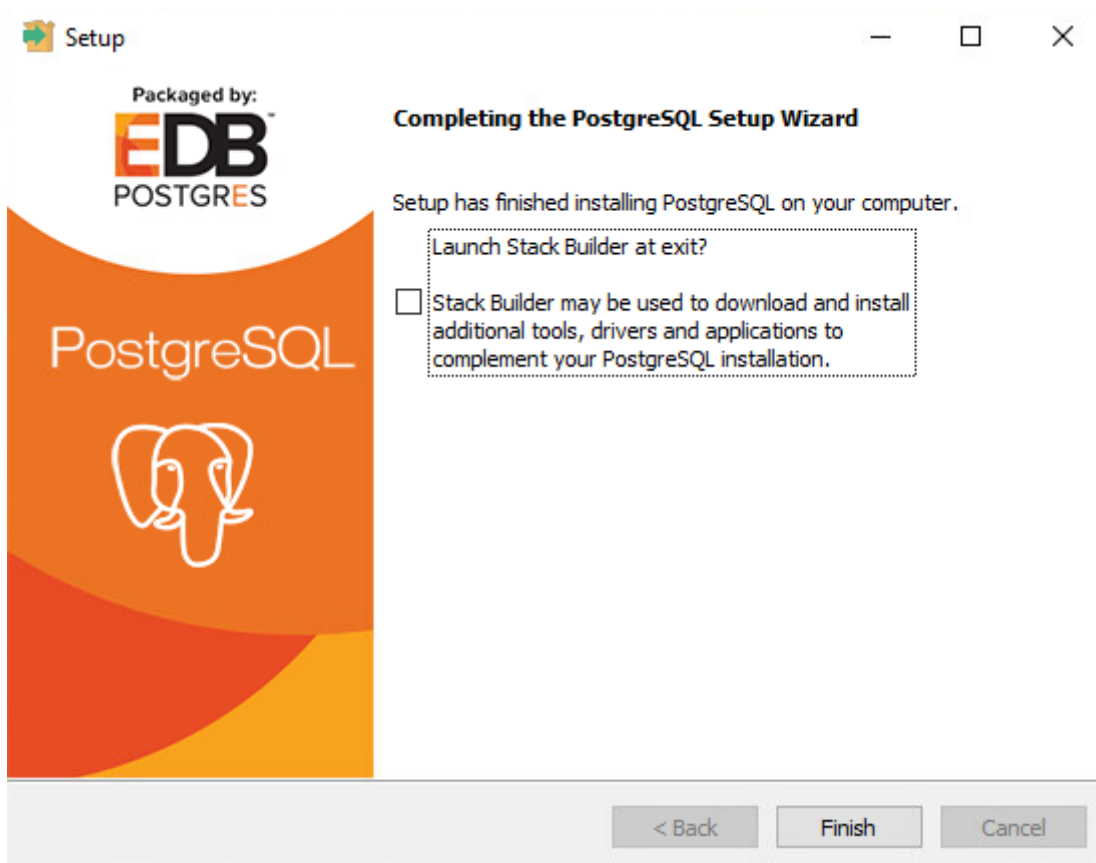
Устанавливаем постгрес.

Вводим пароль:



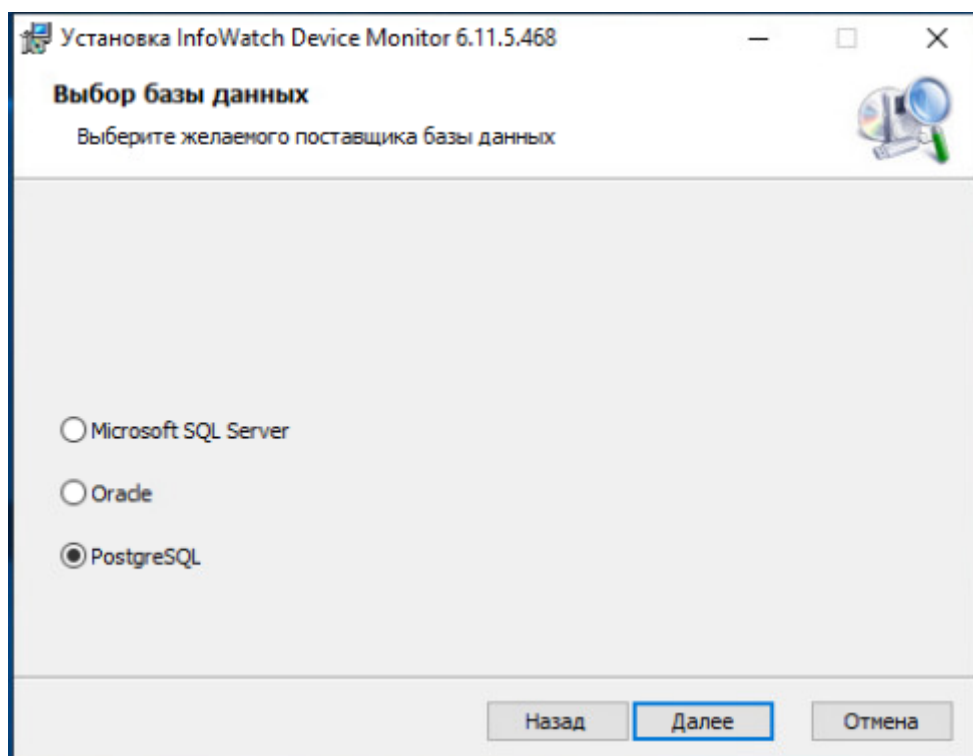
The screenshot shows the 'Password' step of the PostgreSQL Setup Wizard. The window title is 'Setup'. The main heading is 'Password'. Below it, a message says 'Please provide a password for the database superuser (postgres)'. There are two input fields: 'Password' and 'Retype password', both containing seven asterisks. At the bottom right, there is a large green arrow icon pointing right. At the bottom left, the text 'InstallBuilder' is visible. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Всё, по завершению убираем галку:

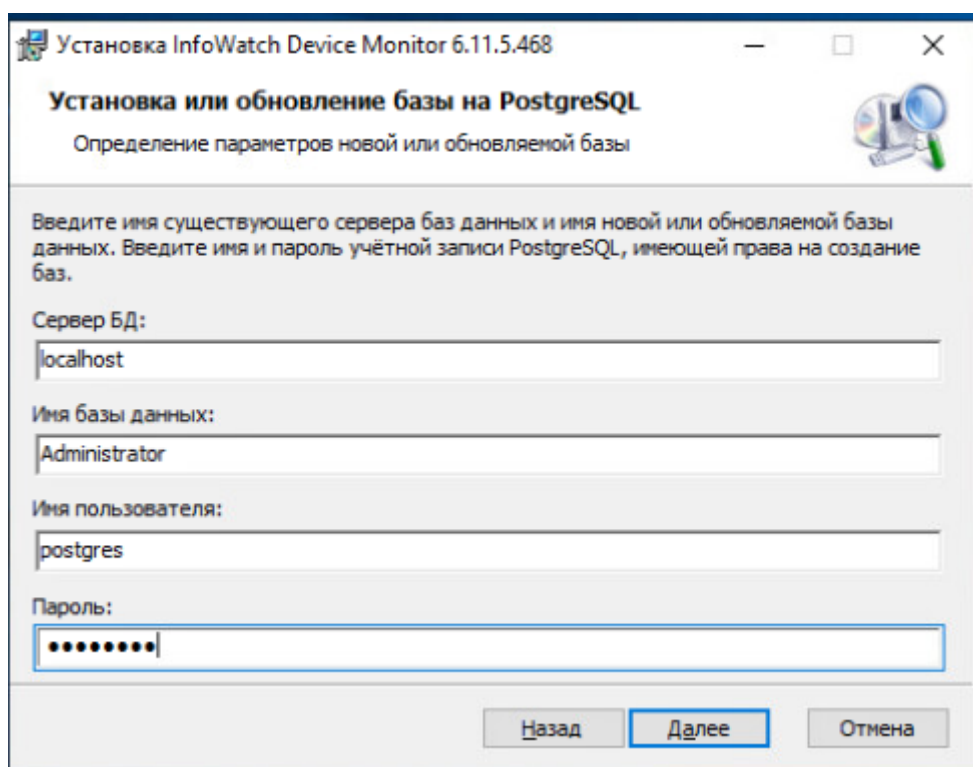


The screenshot shows the 'Completing the PostgreSQL Setup Wizard' screen. The window title is 'Setup'. On the left, there is a large orange graphic with the PostgreSQL logo (an elephant) and the text 'PostgreSQL'. Above the graphic, it says 'Packaged by: EDB POSTGRES'. On the right, the heading is 'Completing the PostgreSQL Setup Wizard'. Below it, a message says 'Setup has finished installing PostgreSQL on your computer.' There is a checkbox labeled 'Launch Stack Builder at exit?'. Below this, a text box explains: 'Stack Builder may be used to download and install additional tools, drivers and applications to complement your PostgreSQL installation.' At the bottom right, there are three buttons: '< Back', 'Finish', and 'Cancel'.

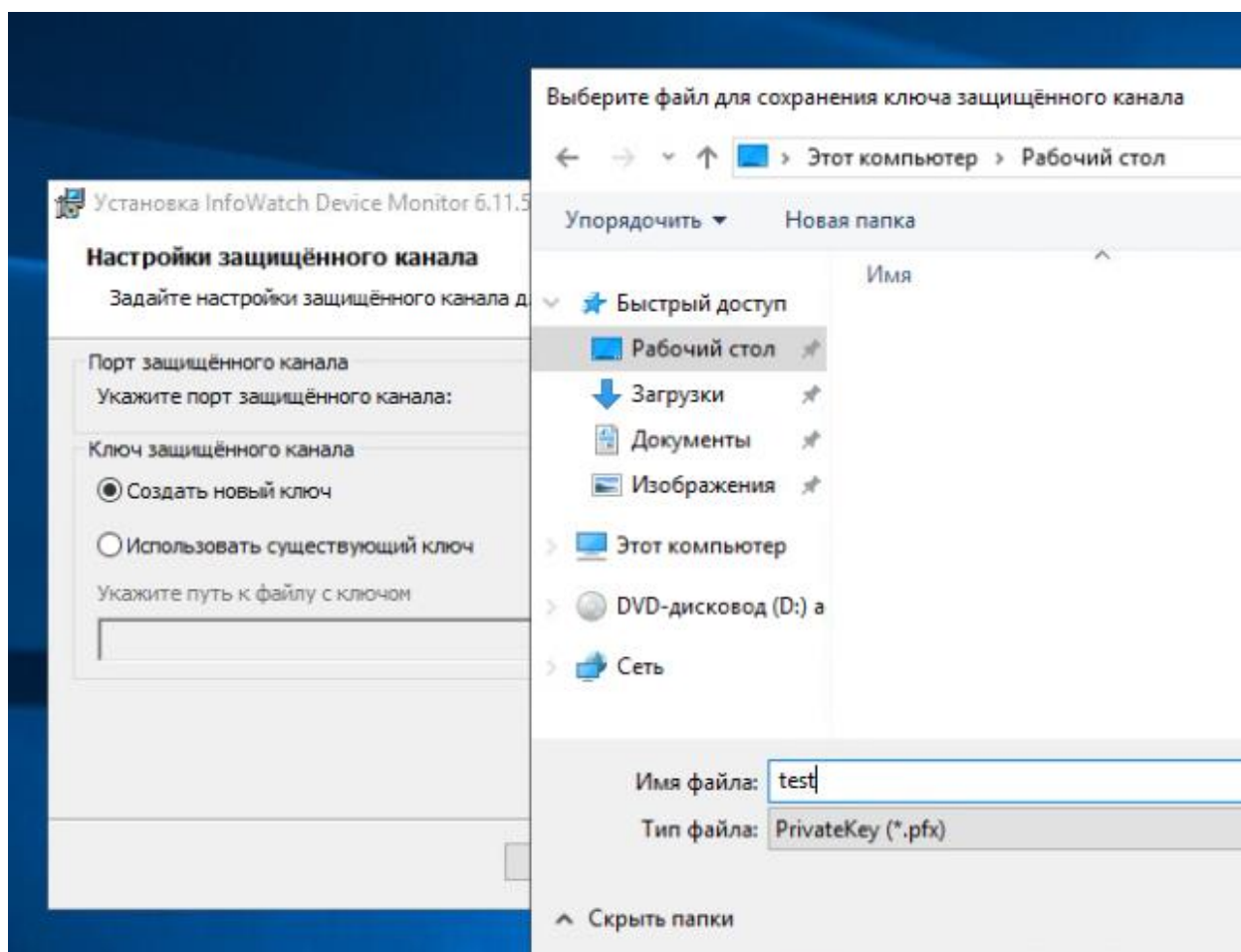
Далее устанавливаем девайс монитор, далее – далее. На этом моменте выбираем это:



А здесь:

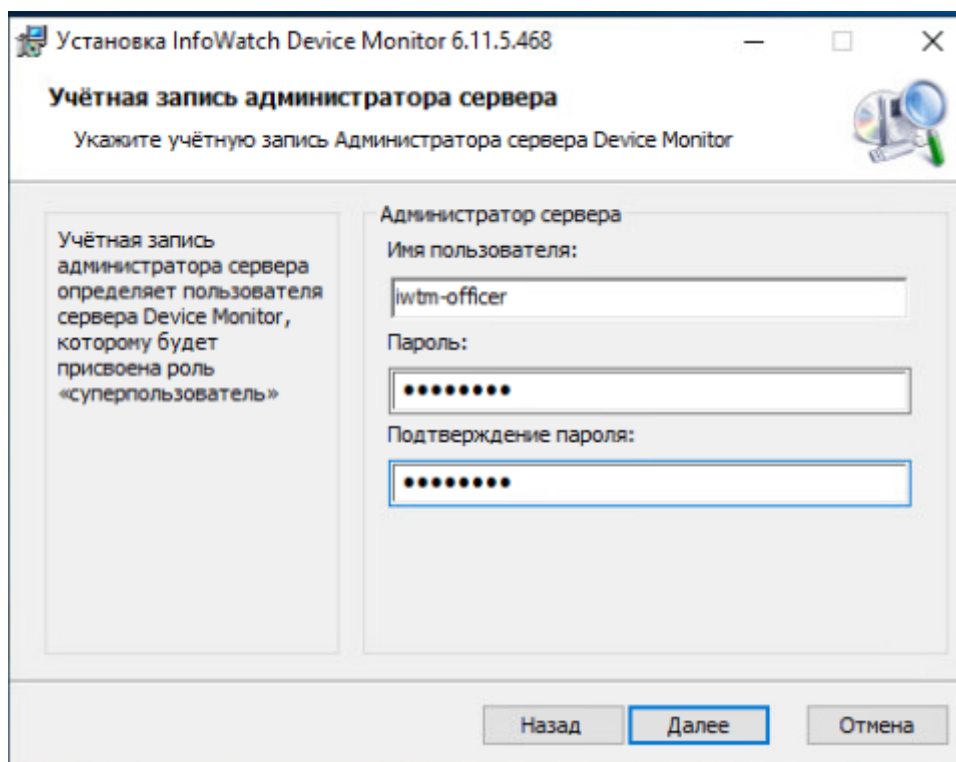


Создаём ключ.



Далее:

Имя юзера пишем "officer"

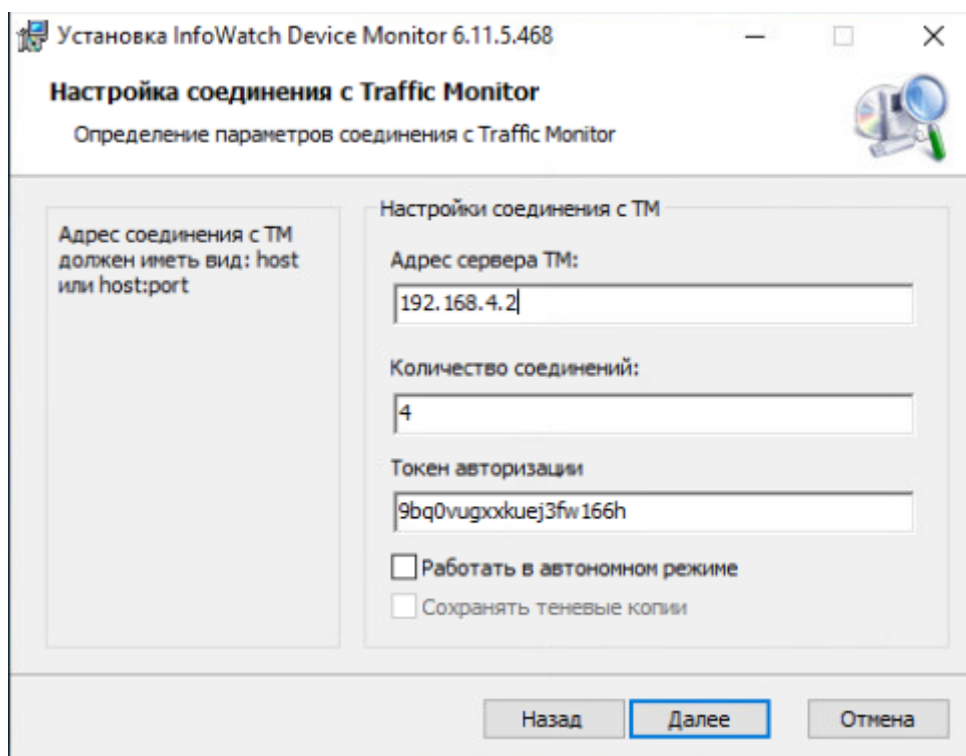


Далее:

Токен ищем здесь:

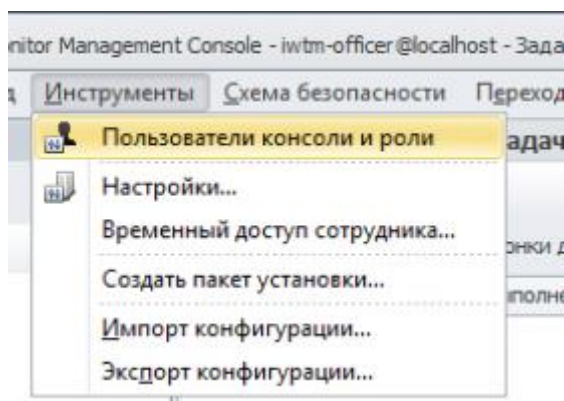
В инфовотче: Управление\плагины\токены

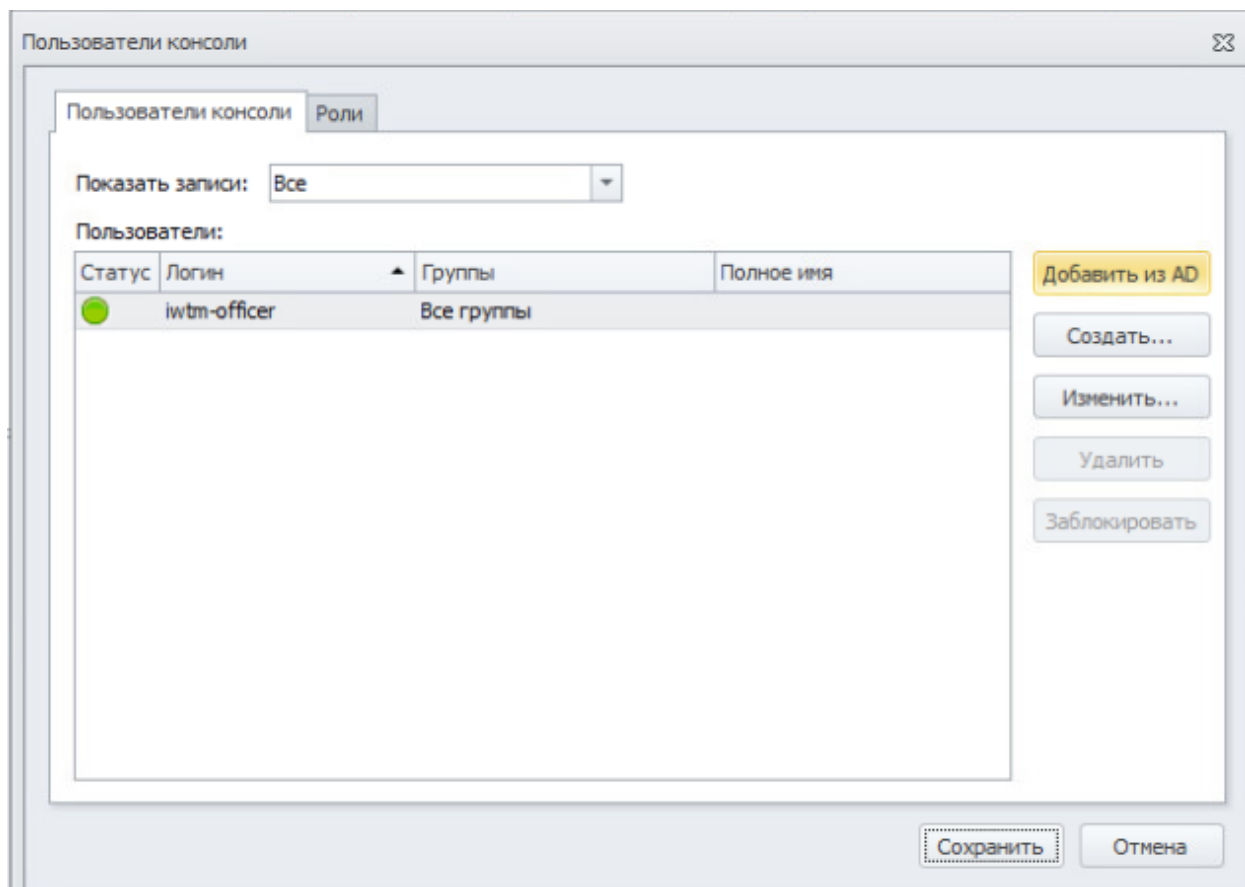
Токены		
	Имя	Содержание
	Token-3	9bq0vugxxkuej3fw166h



После этого заходим в прогу под айви админом вроде:

Подрубаем синхру:





Идем в папки компы и юзеры, у вас может быть по другому

Выдаем такие правила им :

Создание пользователя

✕

Логин: DEMO\Guest

Пароль: *****

Повтор пароля: *****

Полное имя:

Видит сотрудников

Группа сотрудников	Роль пользователя
Группа сотрудников по умолчанию	Офицер безопасности группы

Добавить...

Изменить...

Удалить

Видит компьютеры

Группа компьютеров	Роль пользователя
Группа компьютеров по умолчанию	Офицер безопасности группы

Добавить...

Изменить...

Удалить

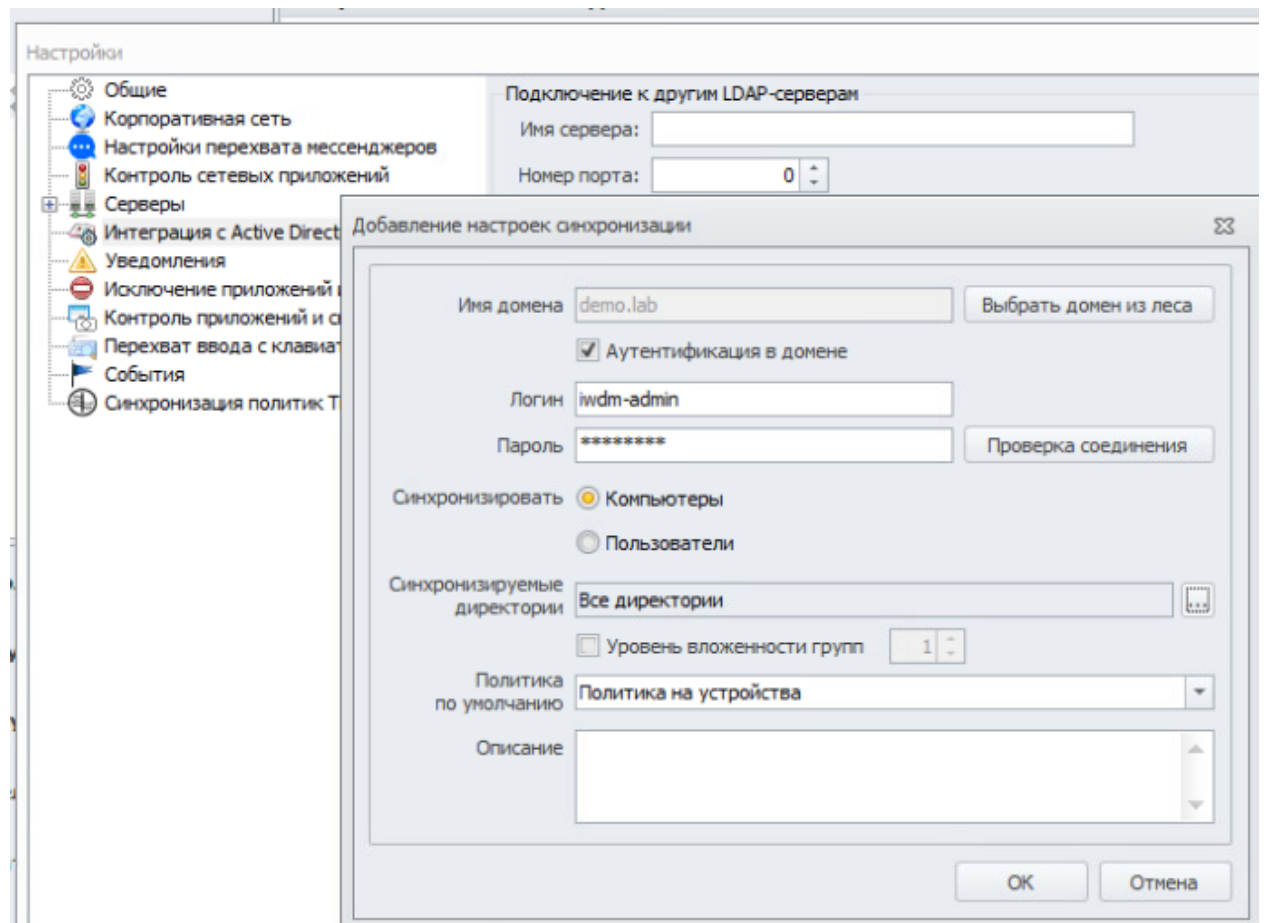
Общие роли

Офицер безопасности	Выбрать
Администратор	Удалить

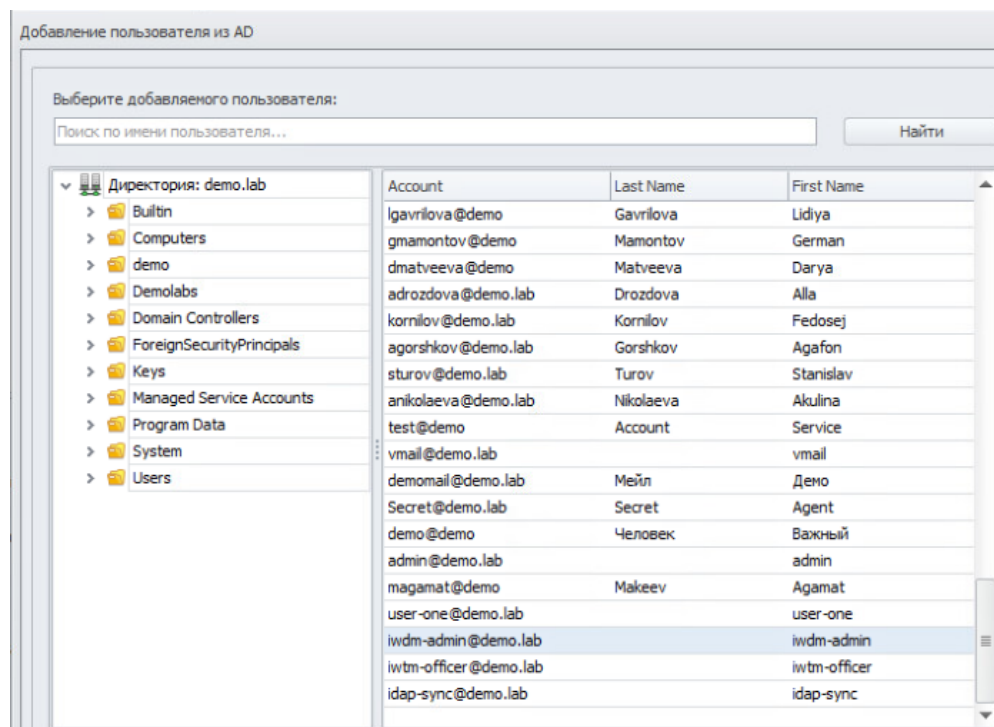
Сохранить

Отмена

Чтобы сделать автоход:



Потом заходим в пользователи и ищем iwdm-admin и добавляем:



Потом раздать все роли:

Создание пользователя

Логин: DEMO\jwdm-admin

Пароль: *****

Повтор пароля: *****

Полное имя: jwdm-admin

Видит сотрудников

Группа сотрудников	Роль пользователя
Группа сотрудников по умолчанию	Офицер безопасности группы

Добавить...
Изменить...
Удалить

Видит компьютеры

Группа компьютеров	Роль пользователя
Группа компьютеров по умолчанию	Офицер безопасности группы

Добавить...
Изменить...
Удалить

Общие роли

Офицер безопасности
Администратор

Выбрать
Удалить

Сохранить Отмена

Запускаем прогу девайс монитор и ставим галочку

InfoWatch Device Monitor Management Console

Адрес сервера: localhost

Логин: DEMO\jwdm-admin

Пароль:

☒ использовать учетные данные текущей сессии Windows

Войти Отмена

Задание 4: Установка агента мониторинга на машине нарушителя

Необходимо ввести клиентскую машину в домен, после перезагрузки войти в систему от ранее созданного пользователя user-one.

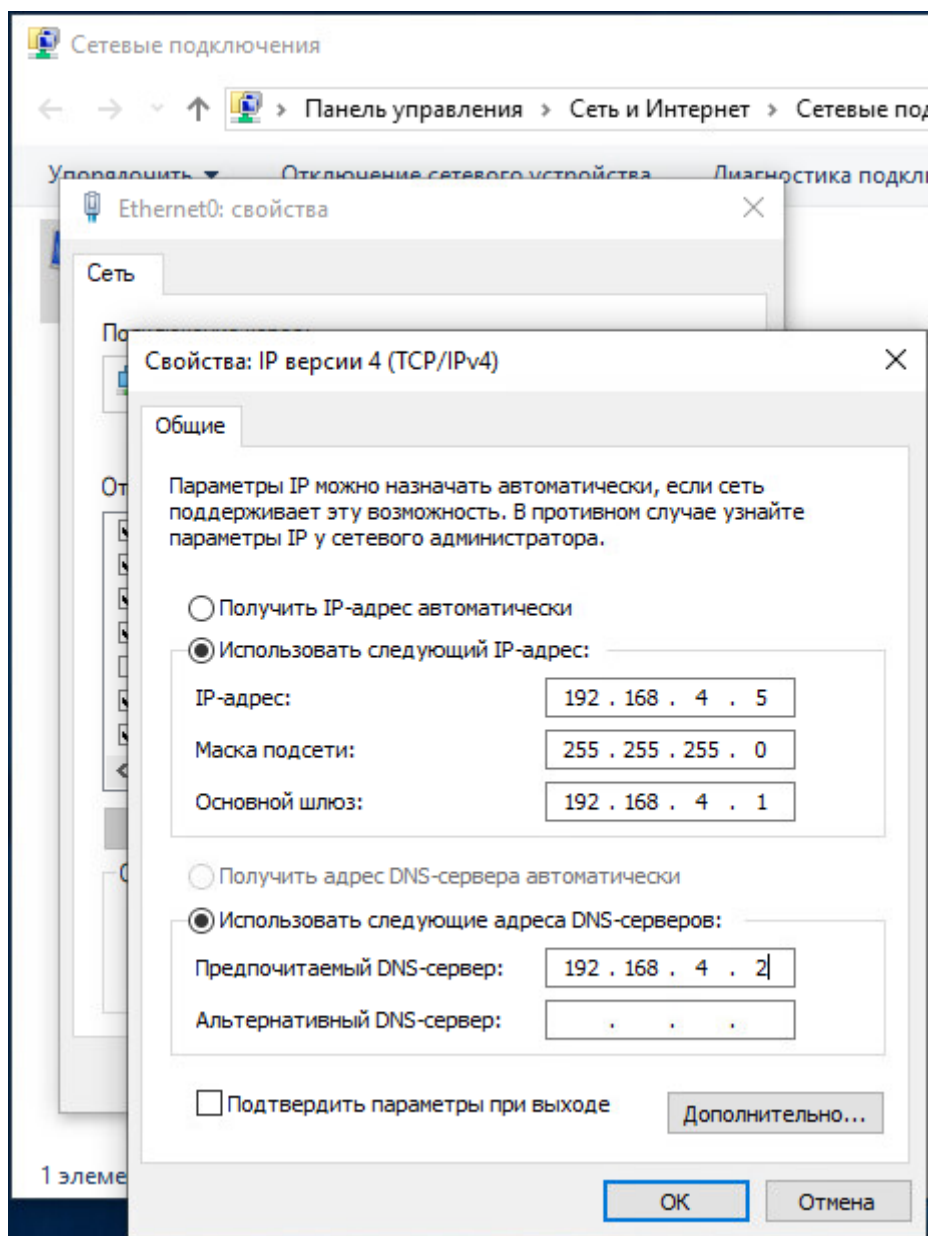
Установить агент мониторинга:

На машину 1 с помощью задачи первичного распространения с сервера агентского мониторинга.

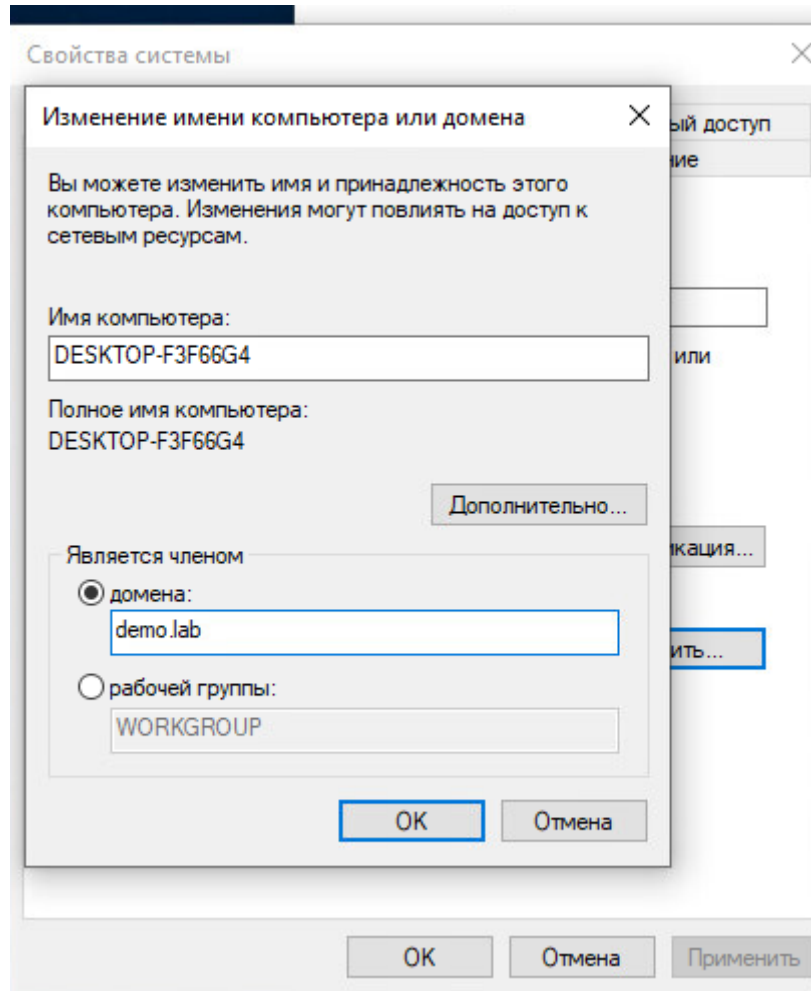
Необходимо создавать отдельные объекты групповых политик на каждое задание и делать снимки экрана для подтверждения создания и выполнения политик.

Ручная установка с помощью переноса на машину нарушителя пакета установки является некорректным выполнением задания!

Для начала:

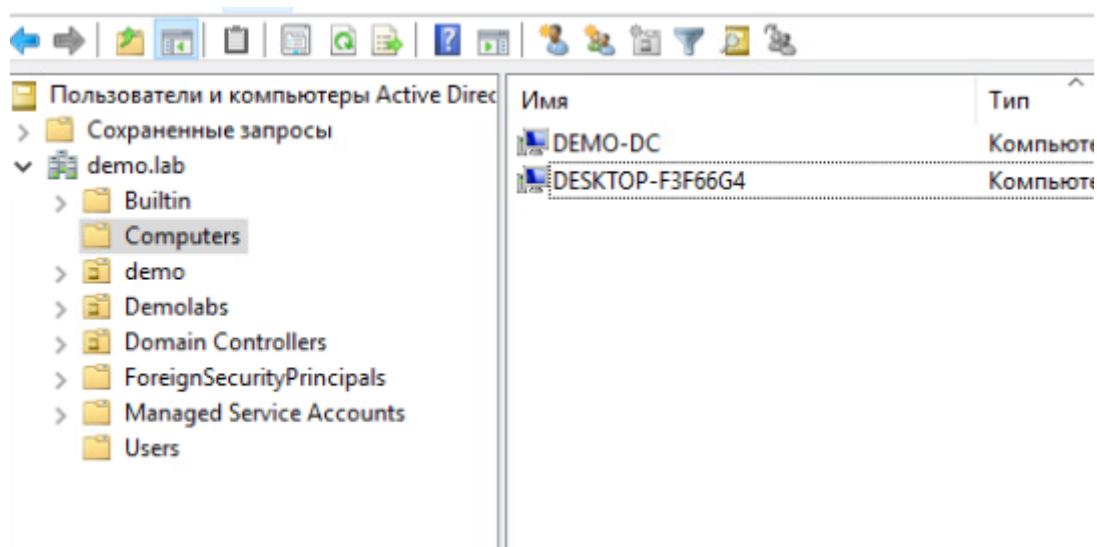


Потом вводим в домен:




После ребута, заходим под user-one

Не забываем переносить ПК в указанную папку. У меня её нет. Оставлю так



Здесь ставим такие галки:

Доменный (текущий профиль) 

Сетевое обнаружение


Если включено сетевое обнаружение, этот компьютер может видеть другие компьютеры и устройства в сети и виден другим компьютерам.


☒ Включить сетевое обнаружение
☐ Отключить сетевое обнаружение

Общий доступ к файлам и принтерам

Если общий доступ к файлам и принтерам включен, то файлы и принтеры, к которым разрешен общий доступ на этом компьютере, будут доступны другим пользователям в сети.

☒ Включить общий доступ к файлам и принтерам
☐ Отключить общий доступ к файлам и принтерам

Все сети 

Все сети 

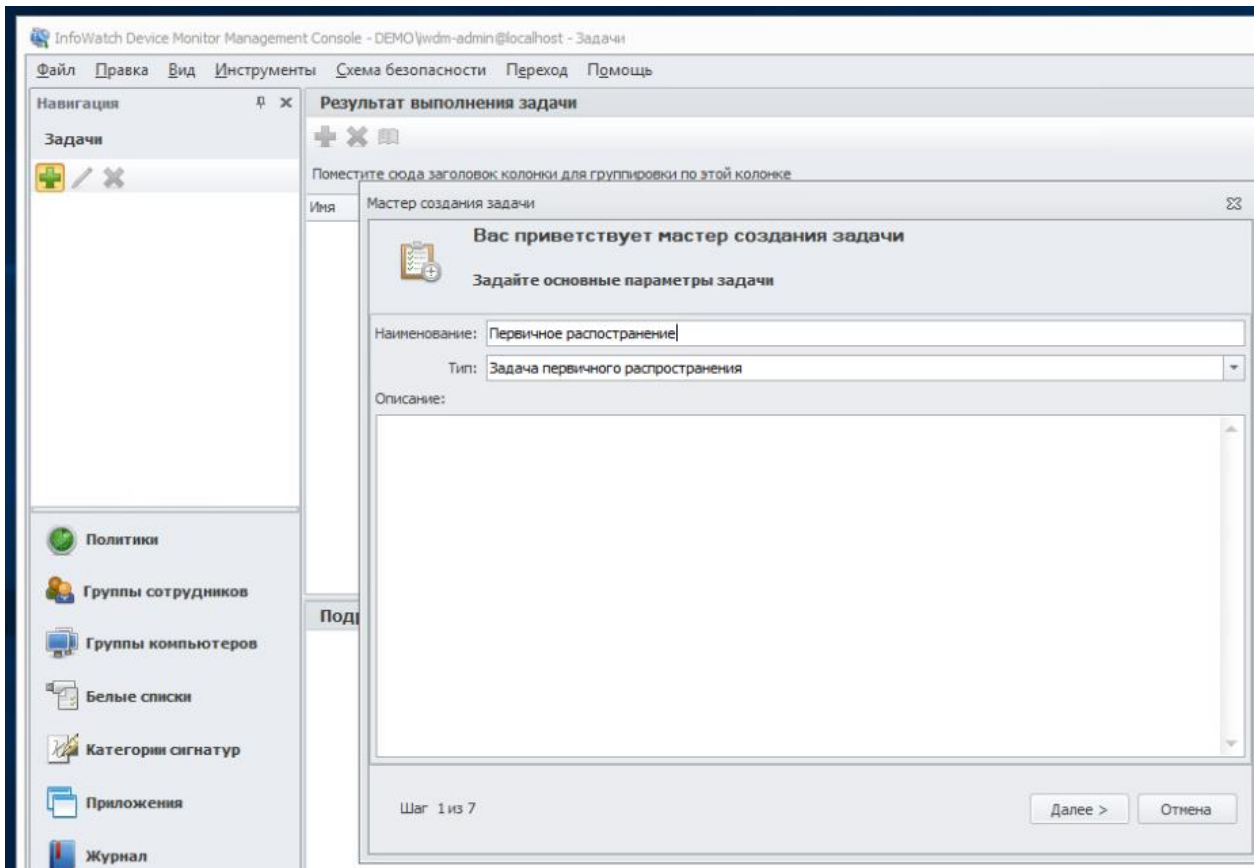
Общий доступ к общедоступным папкам

Если включен общий доступ к общедоступным папкам, пользователи сети (включая членов домашней группы) могут получать доступ к файлам в таких папках.

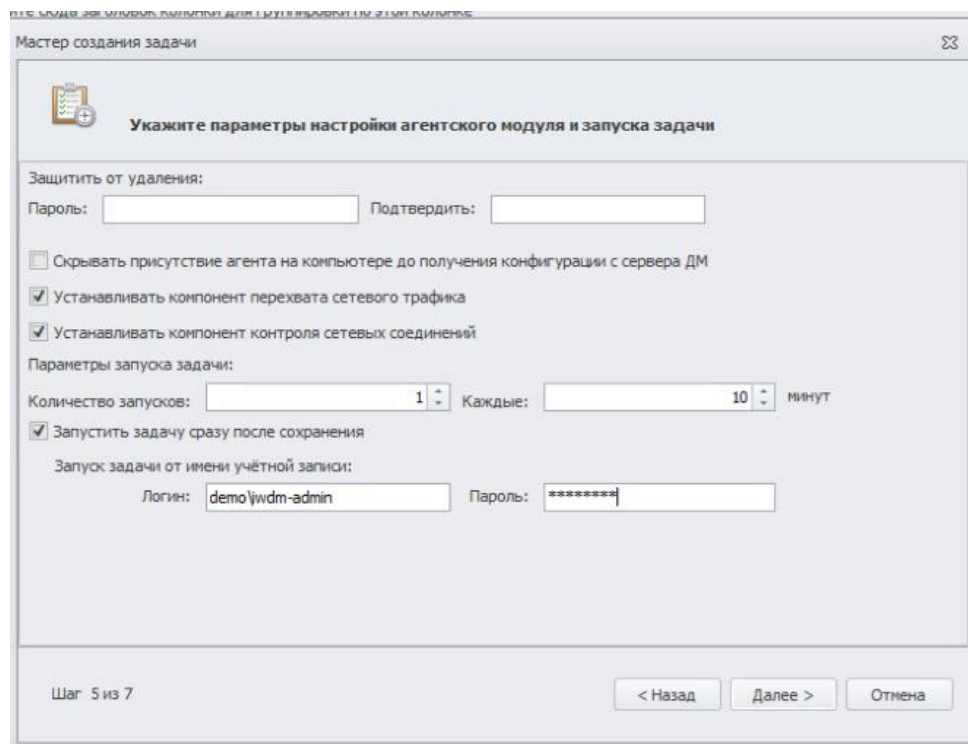
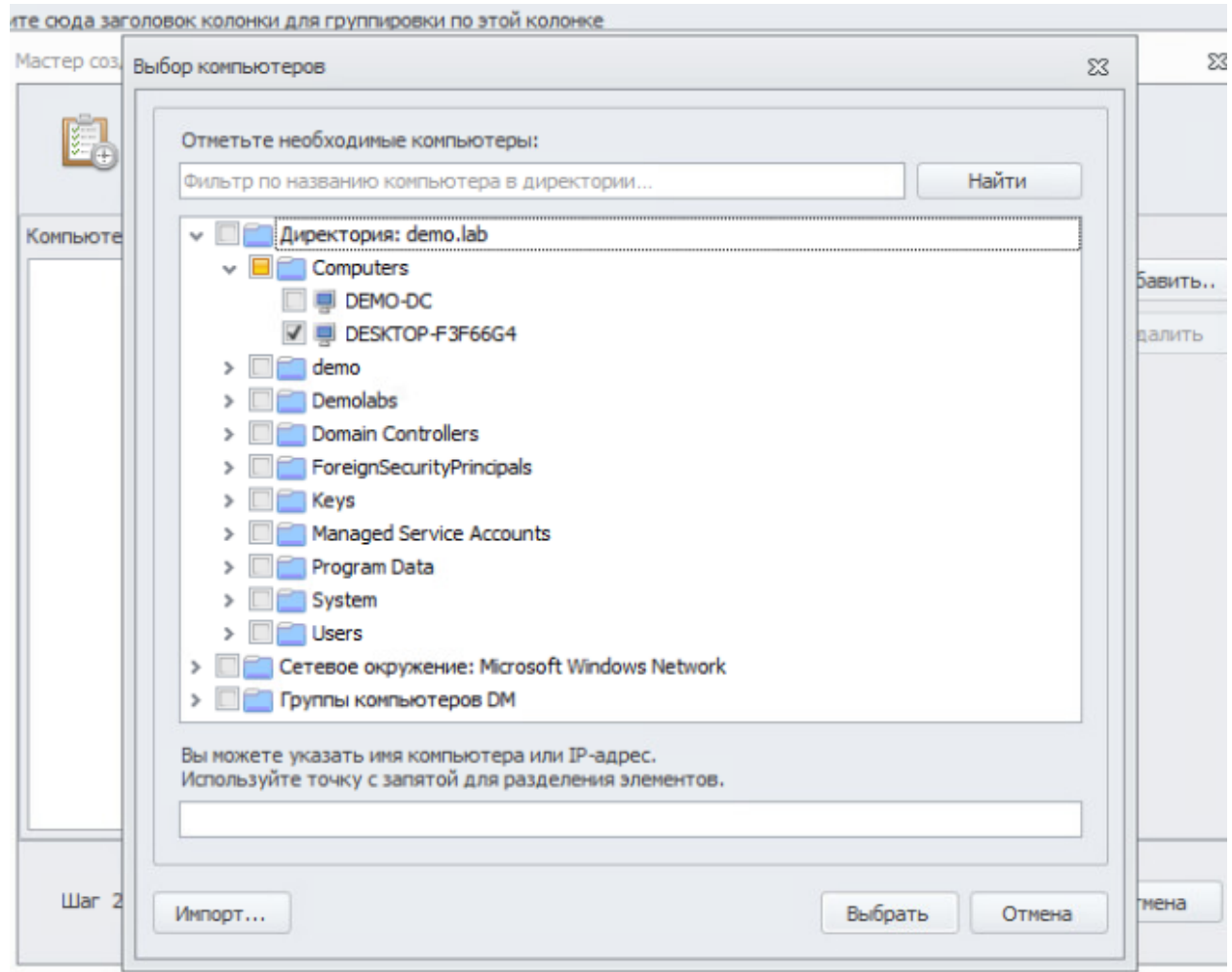
☒ Включить общий доступ, чтобы сетевые пользователи могли читать и записывать файлы в общих папках
☐ Отключить общий доступ (люди, выполнившие вход на этот компьютер, все равно будут иметь доступ к общедоступным папкам)

После этого ребутаем тачку

Пока ребутится такчка, сделаем задачки в iwdm



Далее находим ПК . Чтобы не перепутать чекните названия ПК в клиенте с1



Мастер создания задачи

Укажите параметры перезагрузки

Ожидать перезагрузки без уведомления сотрудника: ☒ Не ожидать
☐ Ожидать 48 час(ов)
☐ Ожидать бесконечно

Уведомлять сотрудника о необходимости перезагрузки и ожидать перезагрузки: ☒ Не уведомлять
☐ Уведомлять в течение 24 час(ов) каждые 10 минут(ы)
☐ Уведомлять бесконечно каждые 10 минут(ы)

Текст уведомления:

☒ Показать предупреждение перед принудительной перезагрузкой

Шаг 6 из 7

< Назад Далее > Отмена

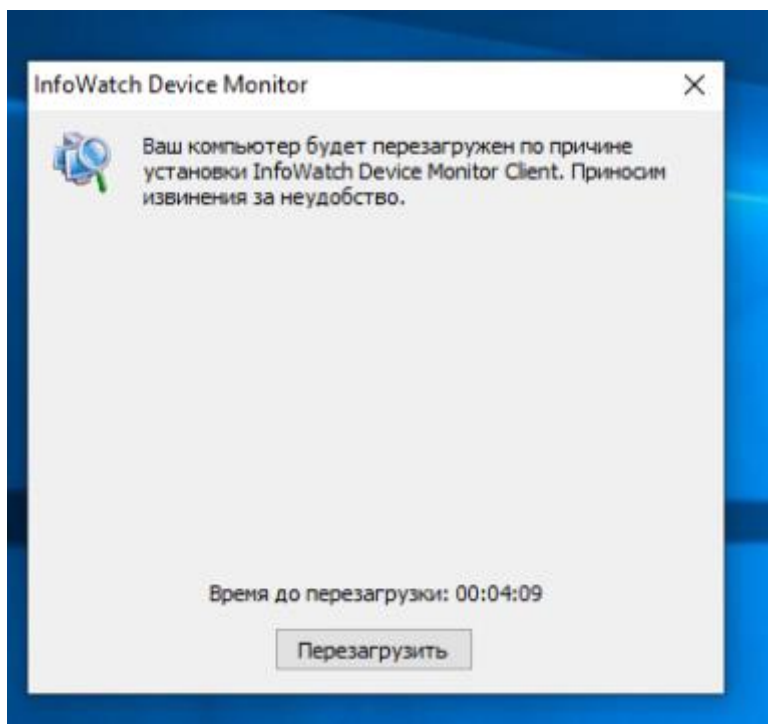
Теперь ждём процесс подготовки

Поместите сюда заголовок колонки для группировки по этой колонке		
Имя	Статус выполнен...	Версия агента
DESKTOP-F3F66G4....	Подготовка	

Ждём такой статус

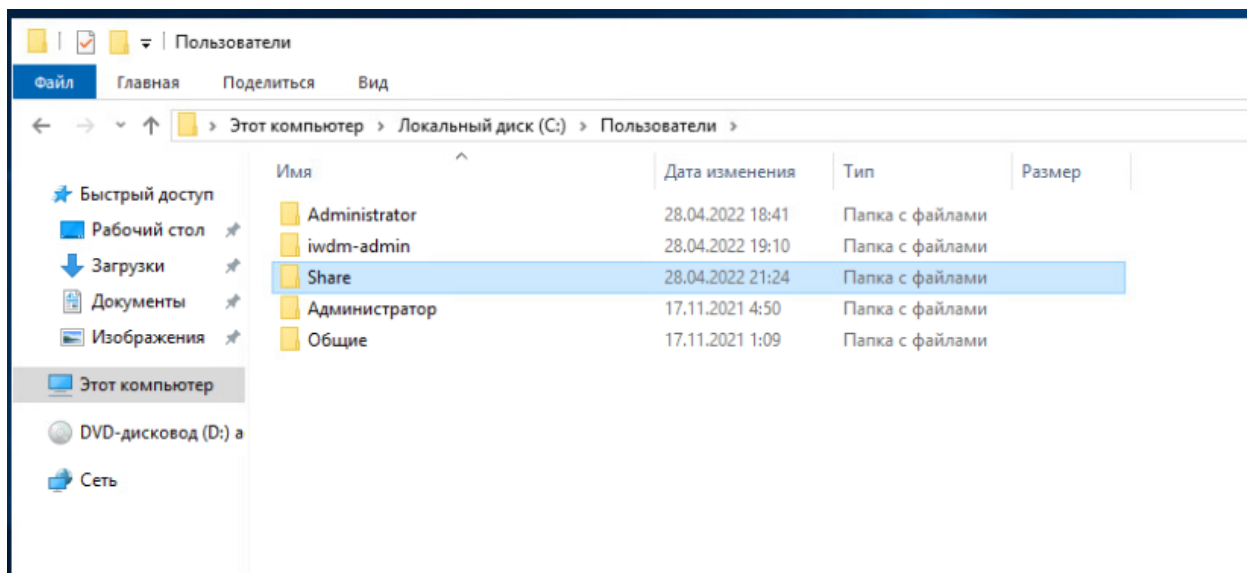
Результат выполнения задачи					
Поместите сюда заголовок колонки для группировки по этой колонке					
Имя	Статус выполнен...	Версия агента	Операционная сис...	Разрядность опер...	К
DESKTOP-F3F66G4....	Ожидание пер...		Windows 10	x64	

У клиента:

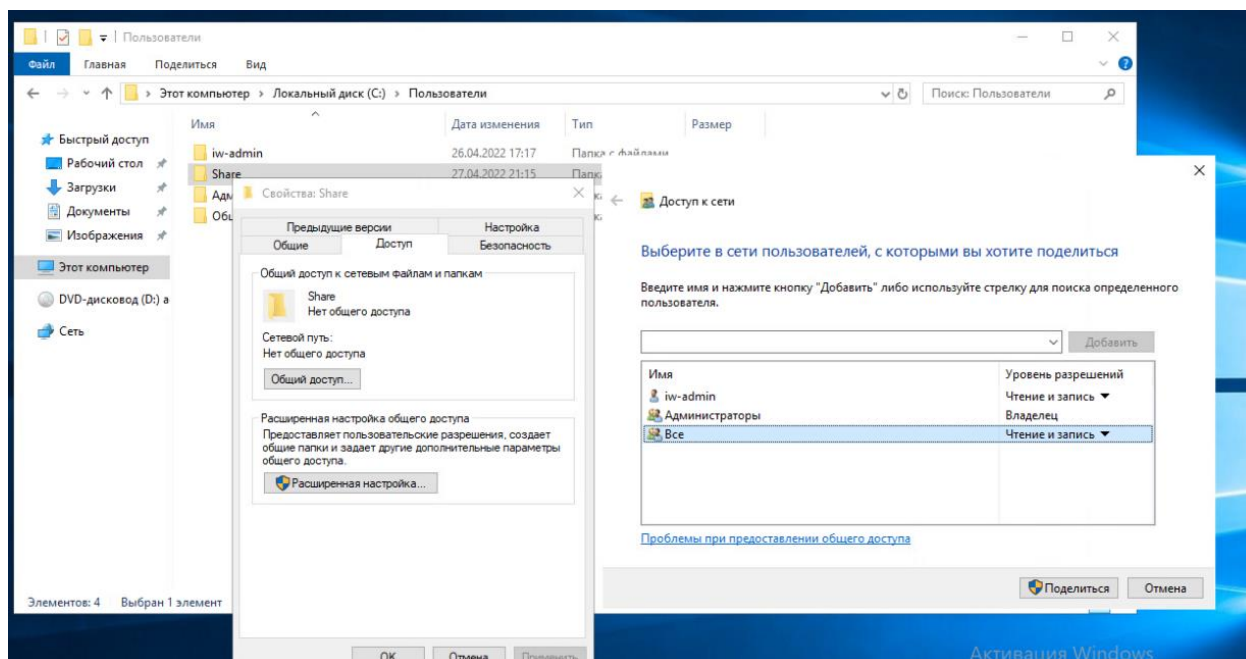


Ребутнули, после этого заходим iwdm.

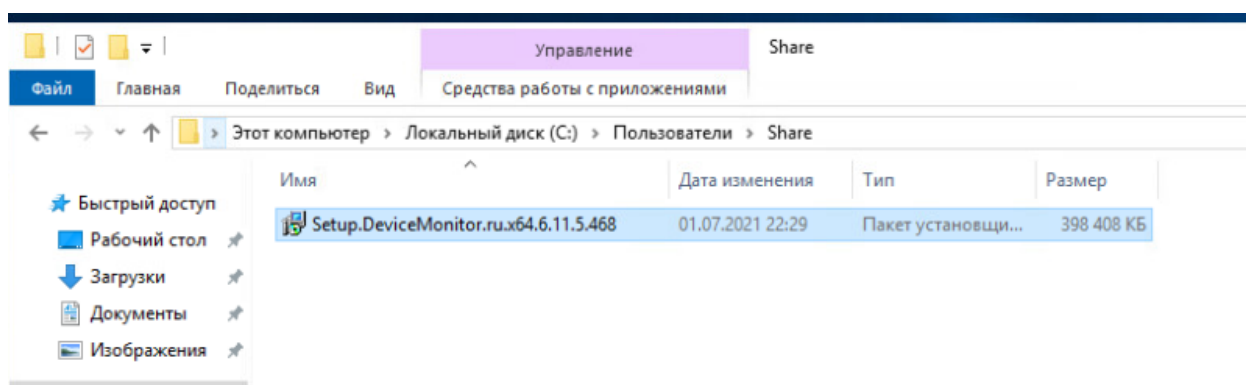
Создаем папку:



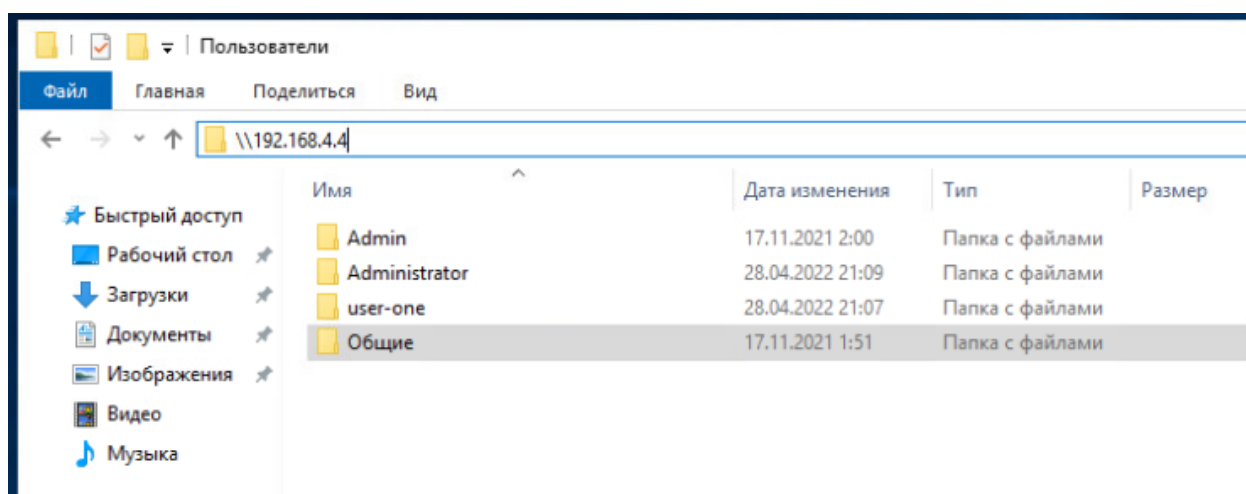
Делаем для всех доступ и добавляем “чтение и запись”.



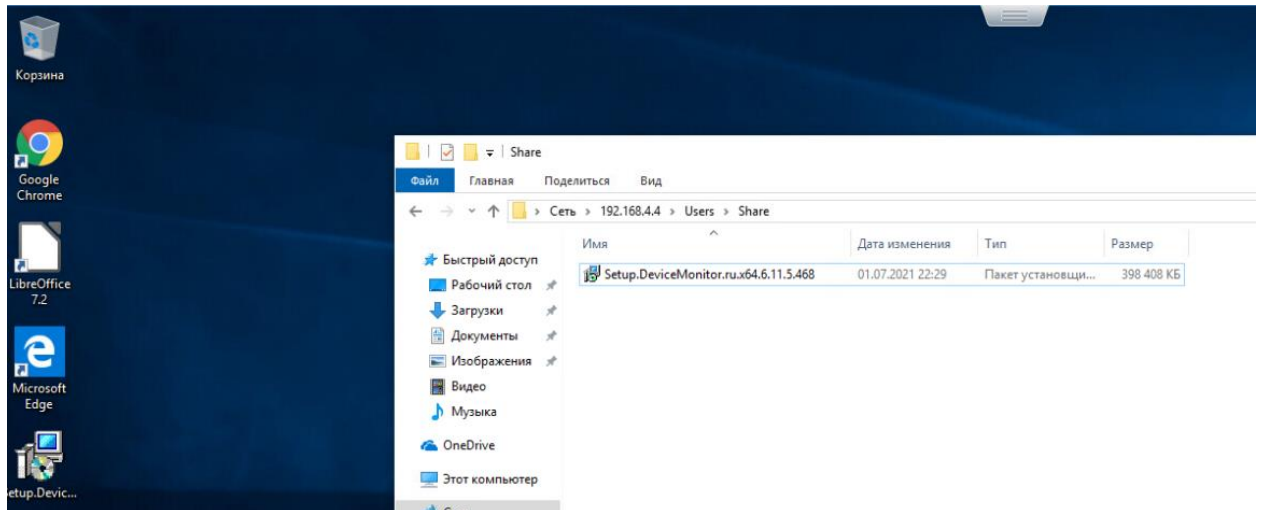
После этого кидаем сетевую папку:



Заходим в клиент и вводим:

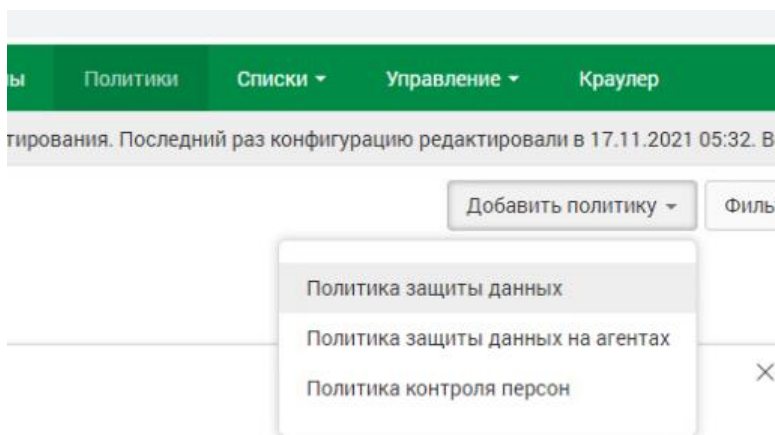


Переносим сетап на рабочий стол.

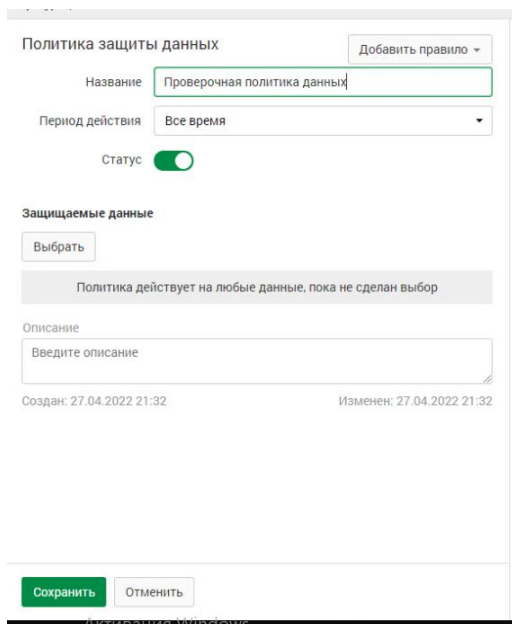


Щас идём в инфо воч.

Добавляем политику защиты данных



Пишем название и сохр "проверочная политика данных "



Далее создаём тег:

Персоны

Политики

Списки

Управление

Краулер

Создать тег

Название

Проверочная политика

Цвет

Описание

Сохранить

Отменить

Заходим в политику добавляем нашему правилу. Ставим в оба направления, меняем уровень и добавляем тег созданный.

Политики

Добавить политику

Фильтр

Политики защиты данных

Проверочная политика данных

Политика на любые данные

Передача

Копирование

Хранение

Работа в приложениях

Добавить правило

Отправители

Направление маршрута

Получатели

Действия

Действия по умолчанию

Любой отправитель

1

Любой получатель

не заданы

не заданы

Договоры и контракты

Каталог объектов защиты: Договоры и контракты

Передача 2

Копирование 1

Хранение

Работа в приложениях

Отдел кадров

Каталог объектов защиты: Отдел кадров

Передача 2

Копирование 1

Хранение

Работа в приложениях

Маркетинг

Правило передачи

Компьютеры

Начните вводить текст

Отправители

Начните вводить текст

Получатели

Начните вводить текст

Дни действия правила

Любой день недели

Часы действия правила

0:00

0:00

Действия при срабатывании правила

Отправить почтовое уведомление

Начните вводить текст

Назначить событие вердикт

Разрешить

Назначить событие уровень нарушения

Низкий

Назначить событие теги

Проверочная политика

Назначить отправителю статус

Выберите статус

Сохранить

Отменить

И так для всех

Передача 1

Копирование

Хранение

Работа в приложениях

Вверху будет окошко :

Применение конфигурации

+ Создание тега Проверочная политика

Атрибут	Значение
Название	Проверочная политика
Цвет	●
Описание	

+ Создание политики Проверочная политика данных

Атрибут	Значение
Название	Проверочная политика данных
Статус	Активная
Тип	Объект
Защищаемые данные	

Применить Закрыть

Конец первого модуля.

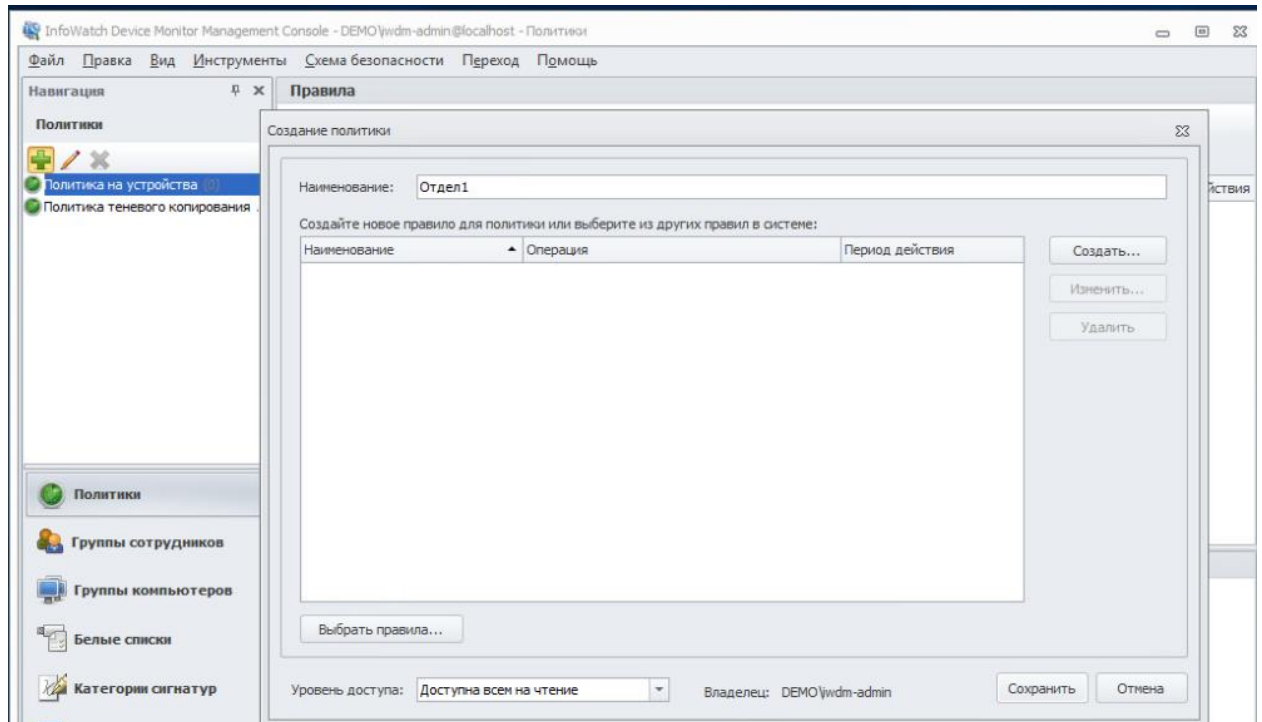
Второй модуль:

Задание 1

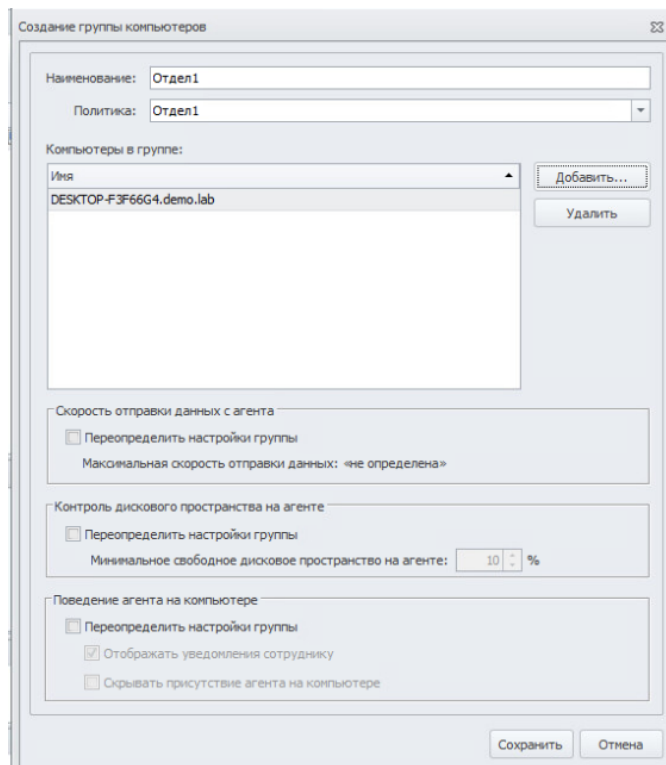
Необходимо создать группу компьютеров: «Отдел1», а также создать новую политику: «Отдел1». Каждая из политик должна применяться только на соответствующие группы. Компьютер 1 необходимо перенести в Отдел1.

Зафиксировать выполнение скриншотом.

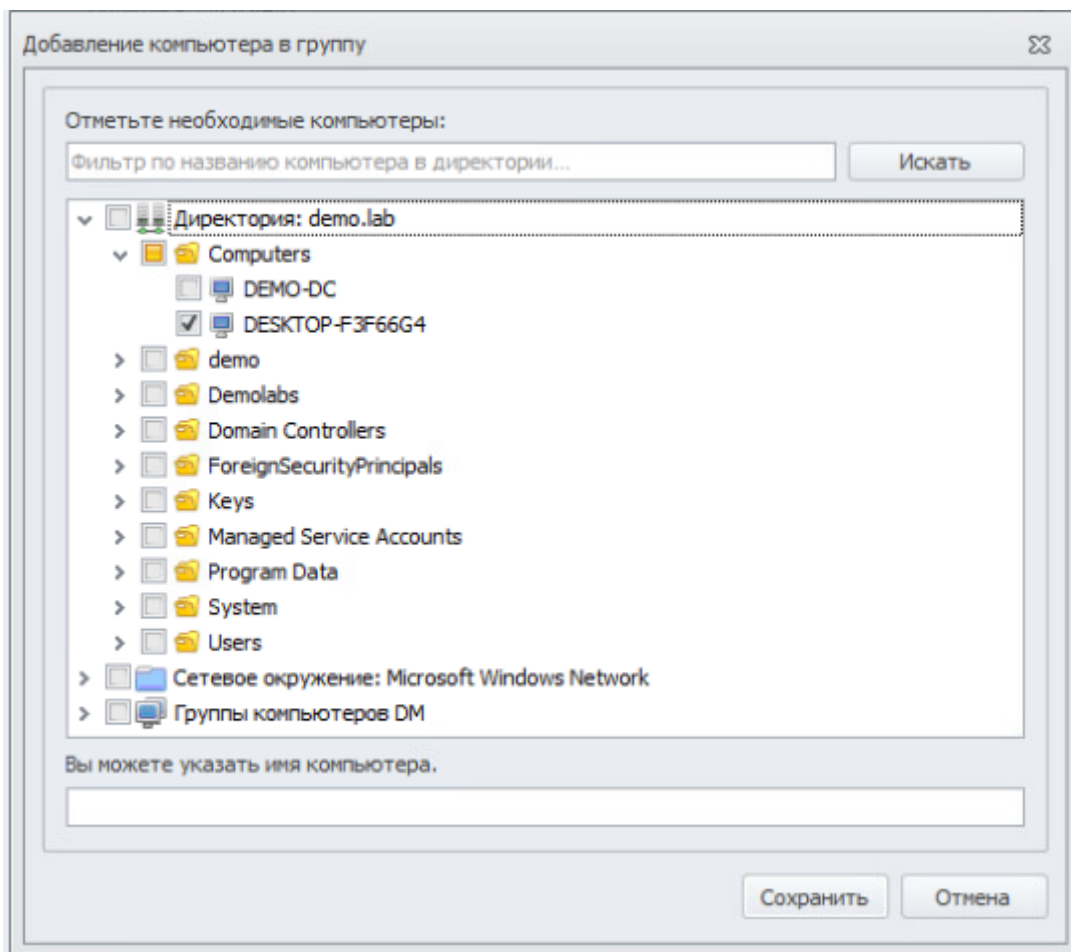
Заходим в iwdm, создаём политику.



Потом создаем группу ПК:



Выбираем ПК клиента c1 и сохраняем.

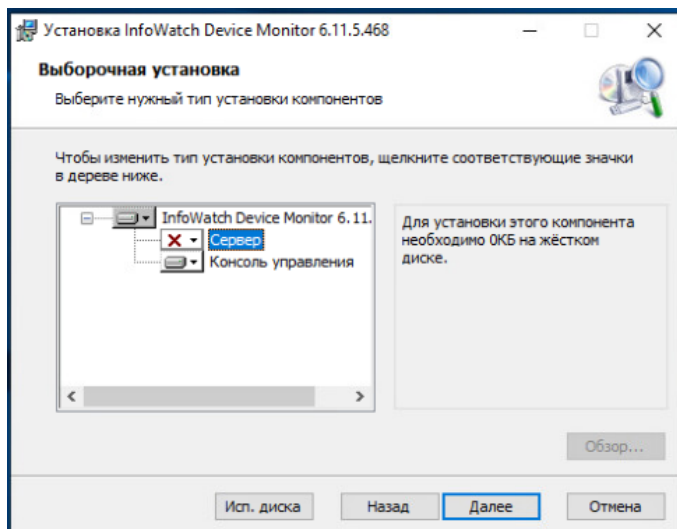
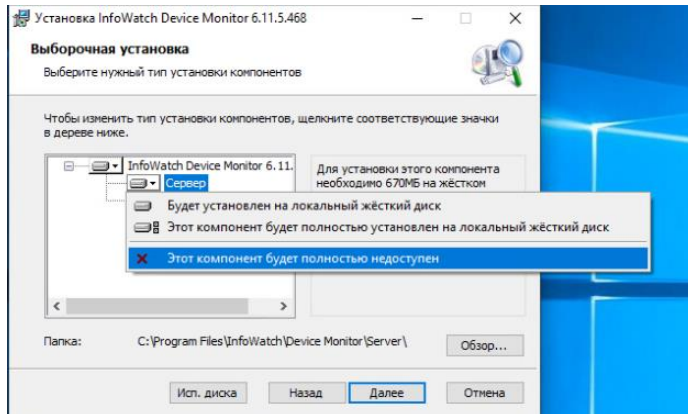


Задание 2

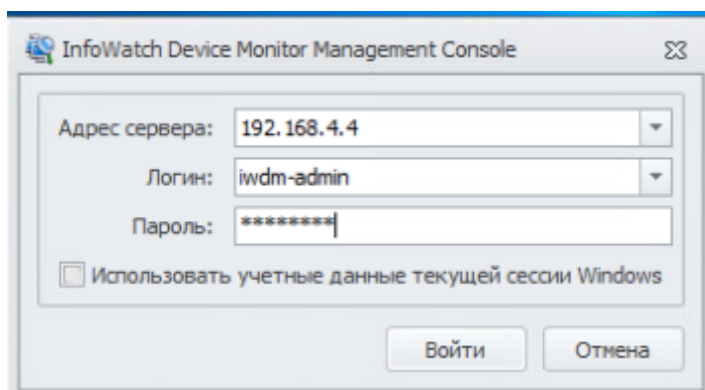
Для удобства работы офицера безопасности необходимо установить дополнительную консоль управления сервером агентского мониторинга на машину W10-agent для удаленного доступа к серверу агентского мониторинга.

Следующие правила создаются в политике «Отдел1».

Устанавливаем на клиент девайс:



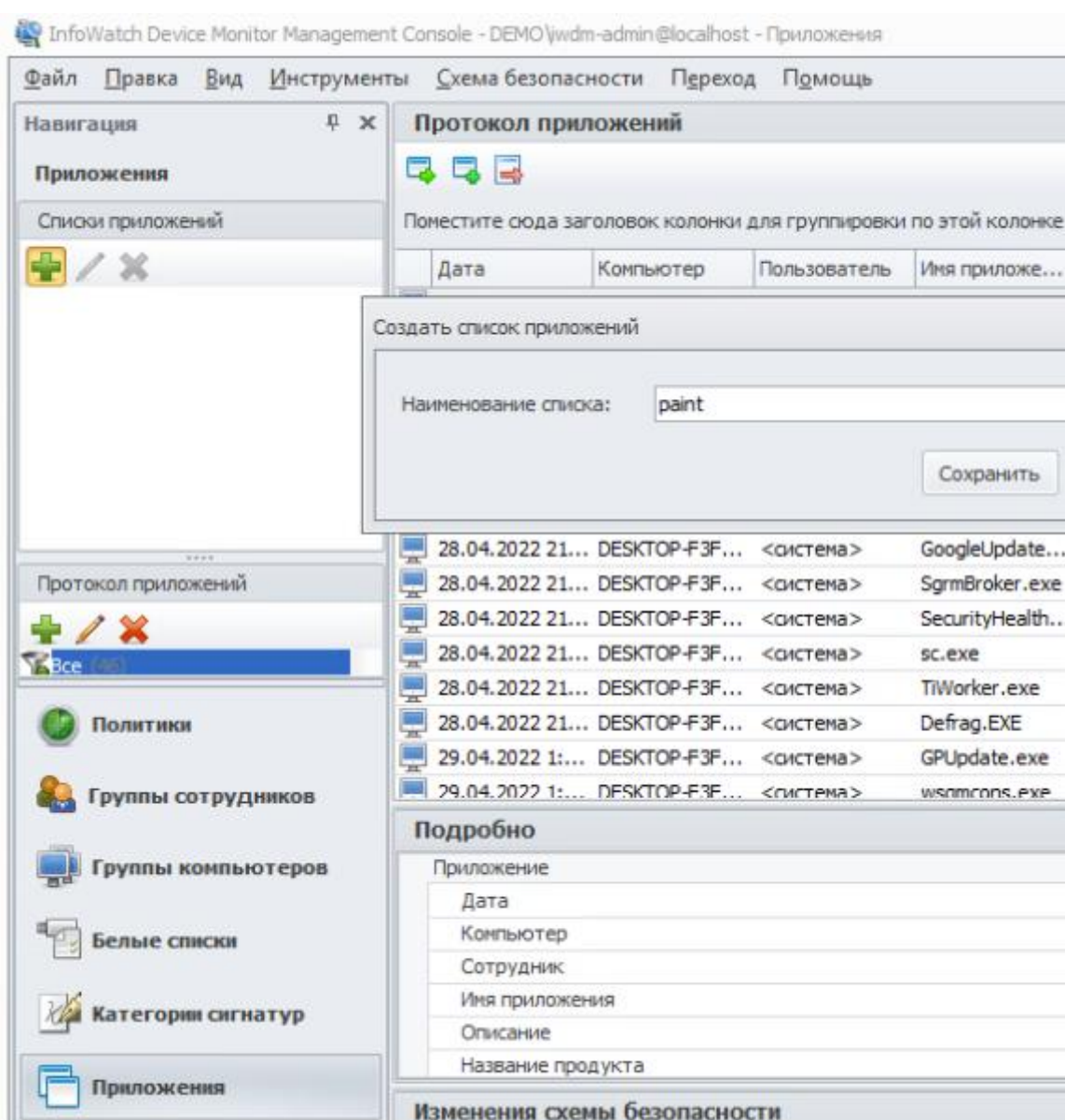
И всё, устанавливаем. Потом идем в консоль.



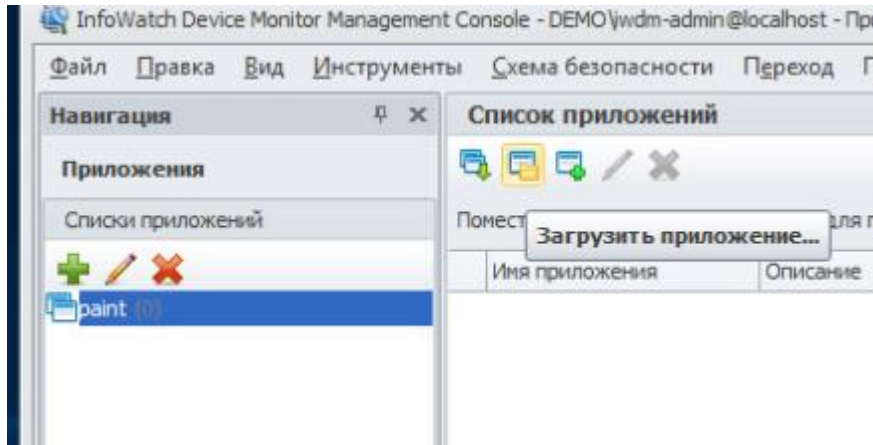
Правило 1

Необходимо запретить пользоваться Microsoft Paint, так как участились случаи подделки печатей компании.

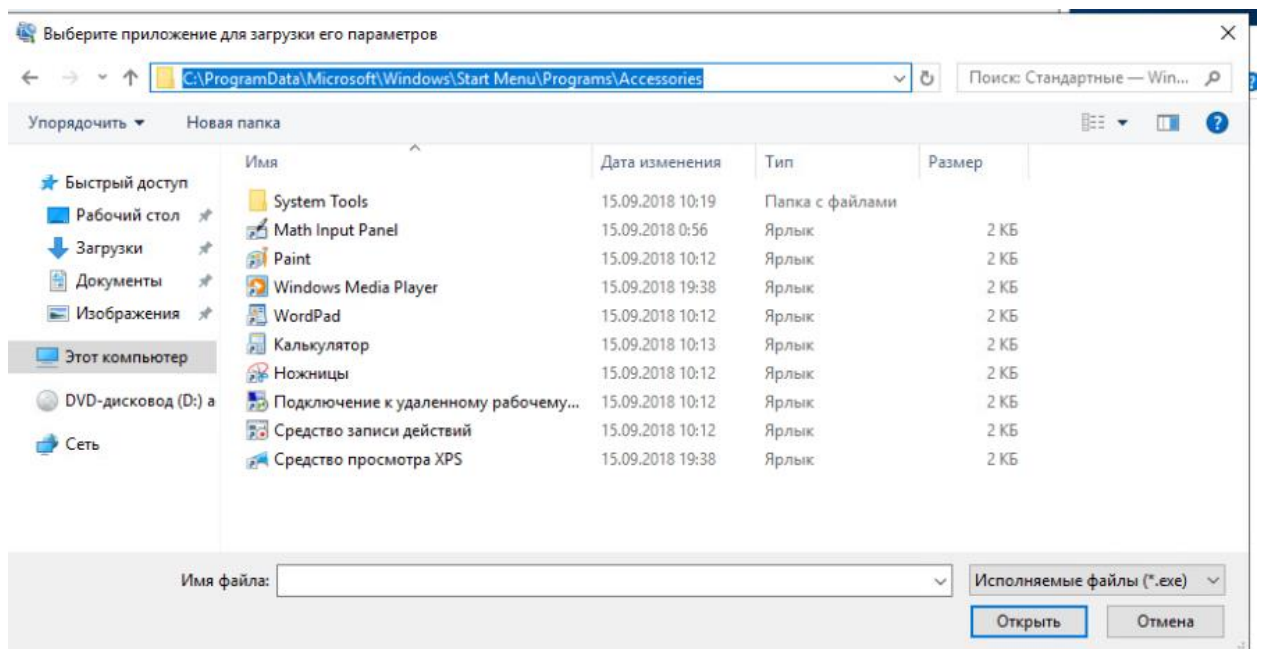
Заходим в iwdm\девайс монитор\приложения\ создаем список приложений



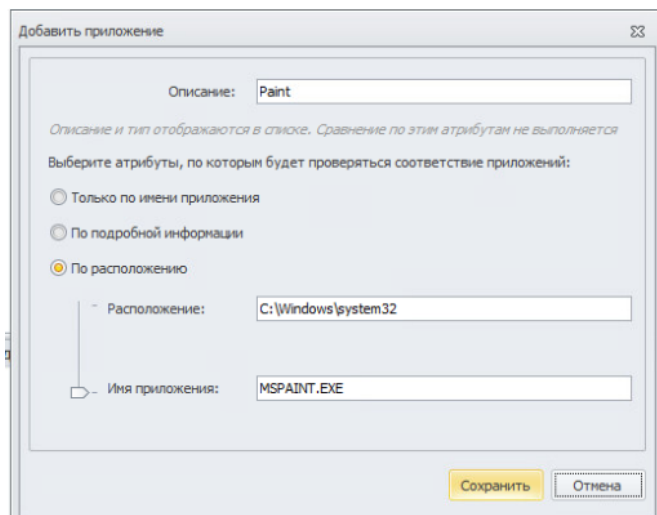
Потом кликаем на желтую херь:



И строке вписываем путь, где лежит пейнт и нажимаем открыть:

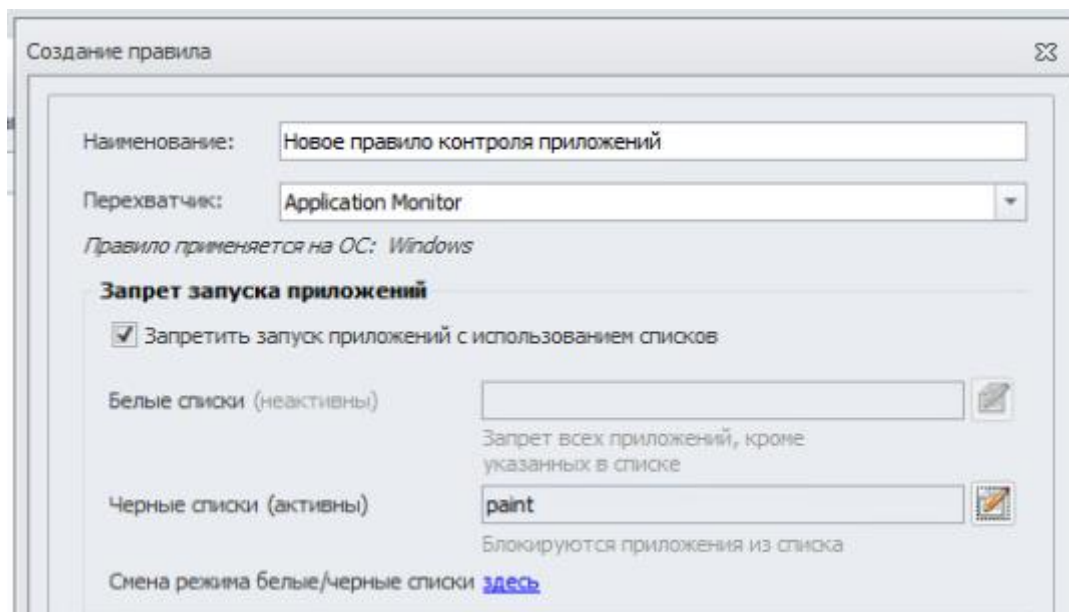


И сохр

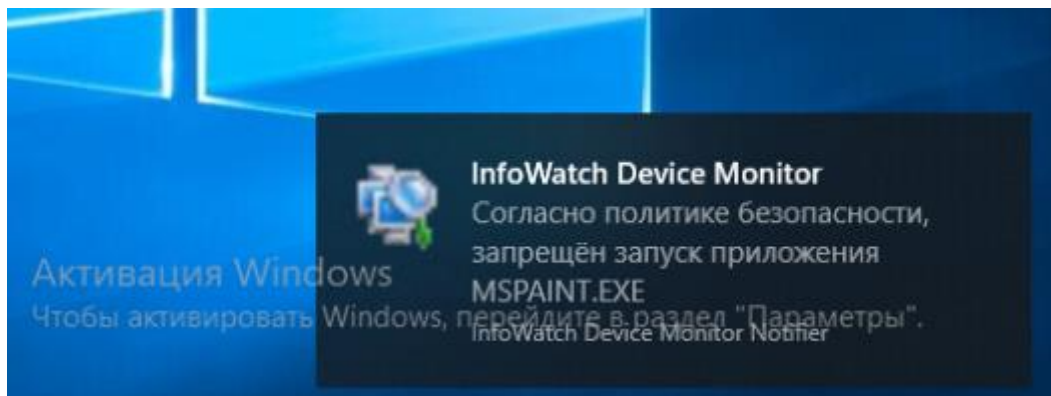
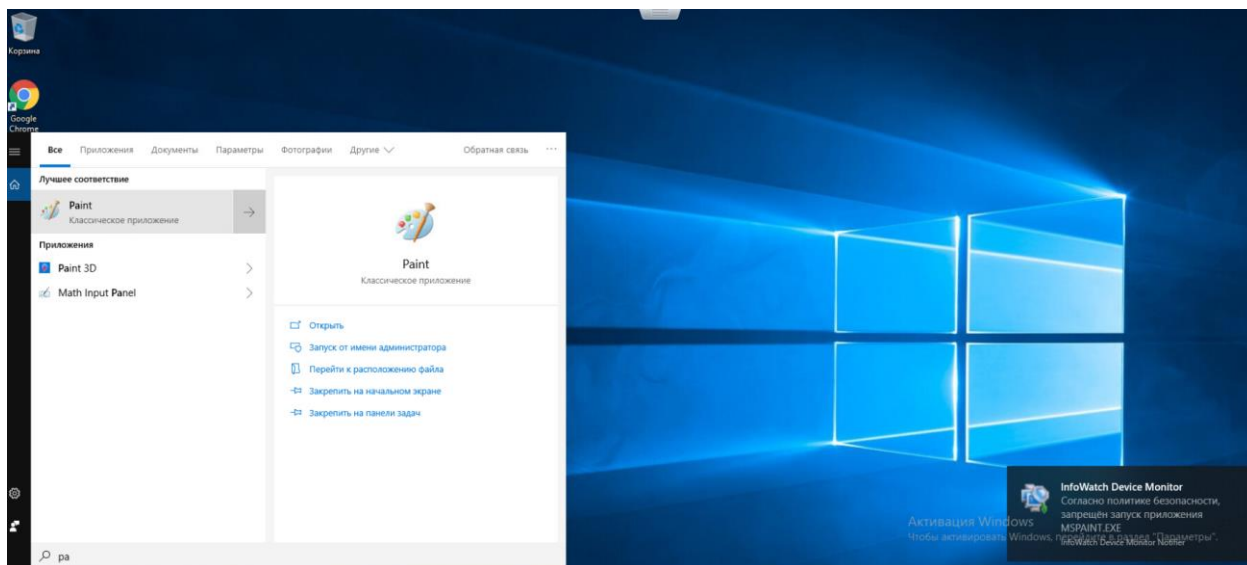


Далее идем в политику, чтобы создать правило на запрет:

В черных списках ищем созданный каталог с пейнтом и сохраняем



И всё вот итог, проверяем у клиента:



Правило 2

Необходимо запретить создание снимков экрана в табличных процессорах для предотвращения утечки секретных расчетов и баз данных.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Создаём новую политику и сохраняем:

Создание правила

Наименование: Новое правило контроля создания снимков экрана

Перехватчик: ScreenShot Control Monitor

Правило применяется на ОС: Windows

Запрещать сотруднику создавать снимок экрана

☒ Всегда

☐ Если запущены приложения: []

☒ Действует всегда

Действует с: [] []

По: [] []

Правило 3

Ограничить доступ к облачным хранилищам GoogleDrive и YandexDisk.

Проверить работоспособность и зафиксировать выполнение.

Создание правила

Наименование: Новое правило контроля облачных хранилищ

Перехватчик: Cloud Storage Monitor

Правило применяется на ОС: Windows, Astra Linux

Настройки доступа к облачным хранилищам

Название	Доступ разрешен	Доступ запрещен	Только скачивание
Google Drive	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
DropBox	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
YandexDisk	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
OneDrive	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
EverNote	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
SugarSync	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Настройки теневого копирования файлов, отправляемых в облачные хранилища

☒ Включить теневое копирование

☒ Минимальный размер файла для создания события: 1 КБ

☒ Максимальный размер теневой копии: 10 240 КБ

☒ Действует всегда

Действует с: [] []

По: [] []

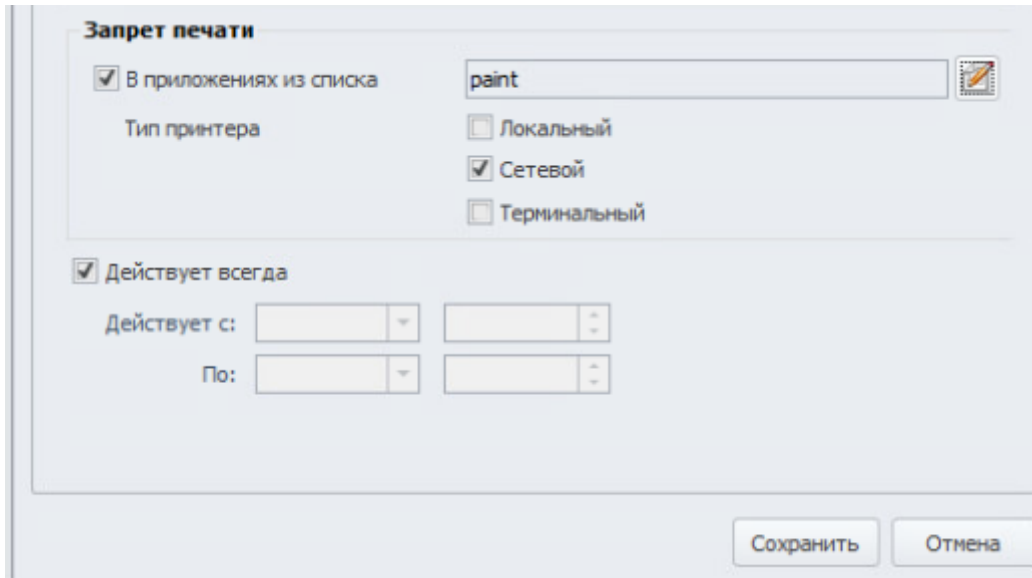
Все так же, выбираем – сохраняем.

Правило 4

Необходимо запретить печать на сетевых принтерах.

Зафиксировать создание политики скриншотом.

В списках можно указать любую папку, можете и создать специально. просто, чтоб дало создать правило.

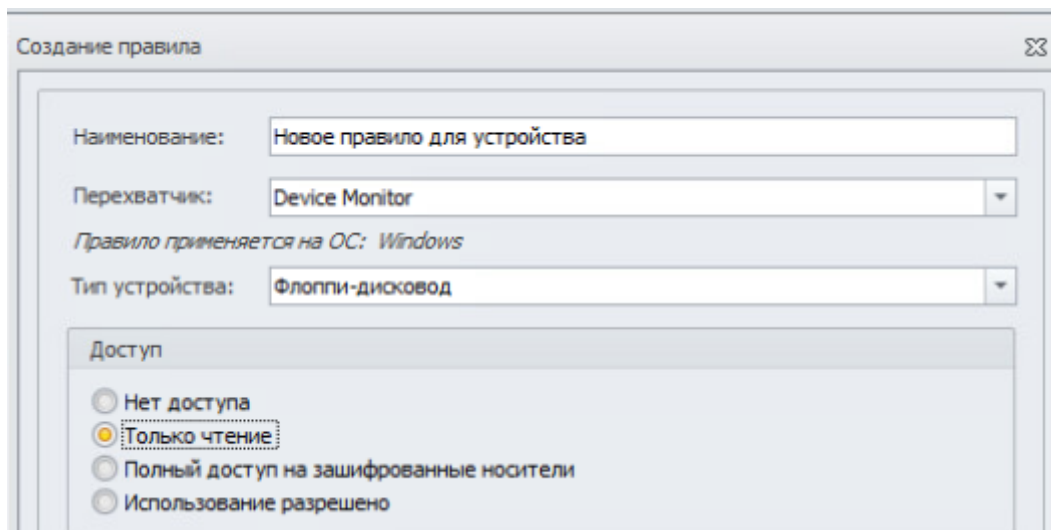


Правило 5

Необходимо запретить запись файлов на все съёмные носители информации, при этом оставить возможность считывания информации.

Проверить работоспособность и зафиксировать выполнение

Создаем правила для каждого компонента:



Создание правила Σ3

Наименование:

Перехватчик:

Правило применяется на ОС: Windows

Тип устройства:

Доступ

☐ Нет доступа
☒ Только чтение
☐ Полный доступ на зашифрованные носители
☐ Использование разрешено

Создание правила X

Наименование:





Перехватчик:

Правило применяется на ОС: Windows

Тип устройства:

Доступ

☐ Нет доступа
☒ Только чтение
☐ Использование разрешено

Новое правило для устройства	 Флоппи-дискет: Только чтение
Новое правило для устройства (1)	 Съемное устройство хранения: Только чтение
Новое правило для устройства (2)	 Терминальное устройство хранения: Только чтение
Новое правило для устройства (3)	 MTP совместимое устройство: Только чтение

Вроде всё запретили.

Правило 6

С учетом ранее созданной блокировки необходимо разрешить использование доверенного носителя информации.

Проверить работоспособность и зафиксировать выполнение

Заходим в белый список и создаем штуку

\Добавить...\ вписываем это:

Добавление устройства в базу

Тип: Другое устройство USB

Идентификатор: USB\VID_3333 Проверить

Описание:

Сохранить Отмена

Отметить все
Сбросить все
Добавить...
Редактировать...
Удалить
Найти...

Мы создали доверенную флешку:

Это итог, скринить это надо:

Создание белого списка

Отметьте разрешенные устройства:

Тип ▲

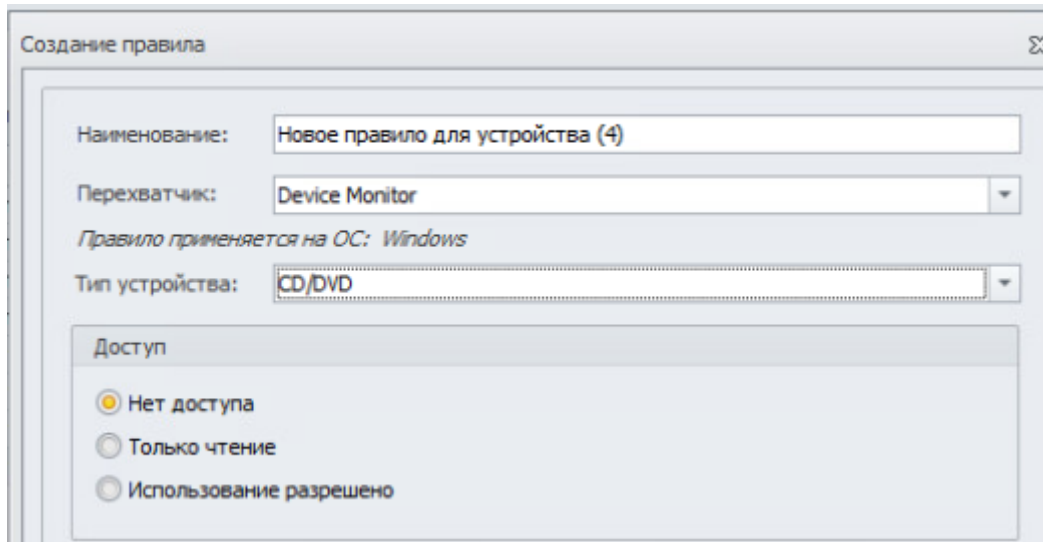
Категория	Описание устройства	Идентификатор устройства	Добавлен	Компьютер
▼ Тип: Другое устройство USB				
<input checked="" type="checkbox"/> Модель		USB\VID_3333	29.04.2022 13:09:19	

Отметить все
Сбросить все
Добавить...
Редактировать...
Удалить
Найти...

Правило 7

Полностью запретить использование CD/DVD-дискового.

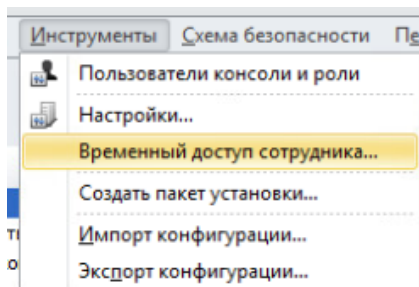
Проверить работоспособность и зафиксировать выполнение



Правило 8

С учетом ранее выполненного запрета необходимо предоставить временный доступ для устройства на 7 минут для пользователя.

Зафиксировать этапы выдачи доступа и работоспособность скриншотами.



Было сказано на 7мин, но это такого критерия нет, поэтому ставим минималку в 30мин...

