

# MS Windows XP & 2003 SNMP

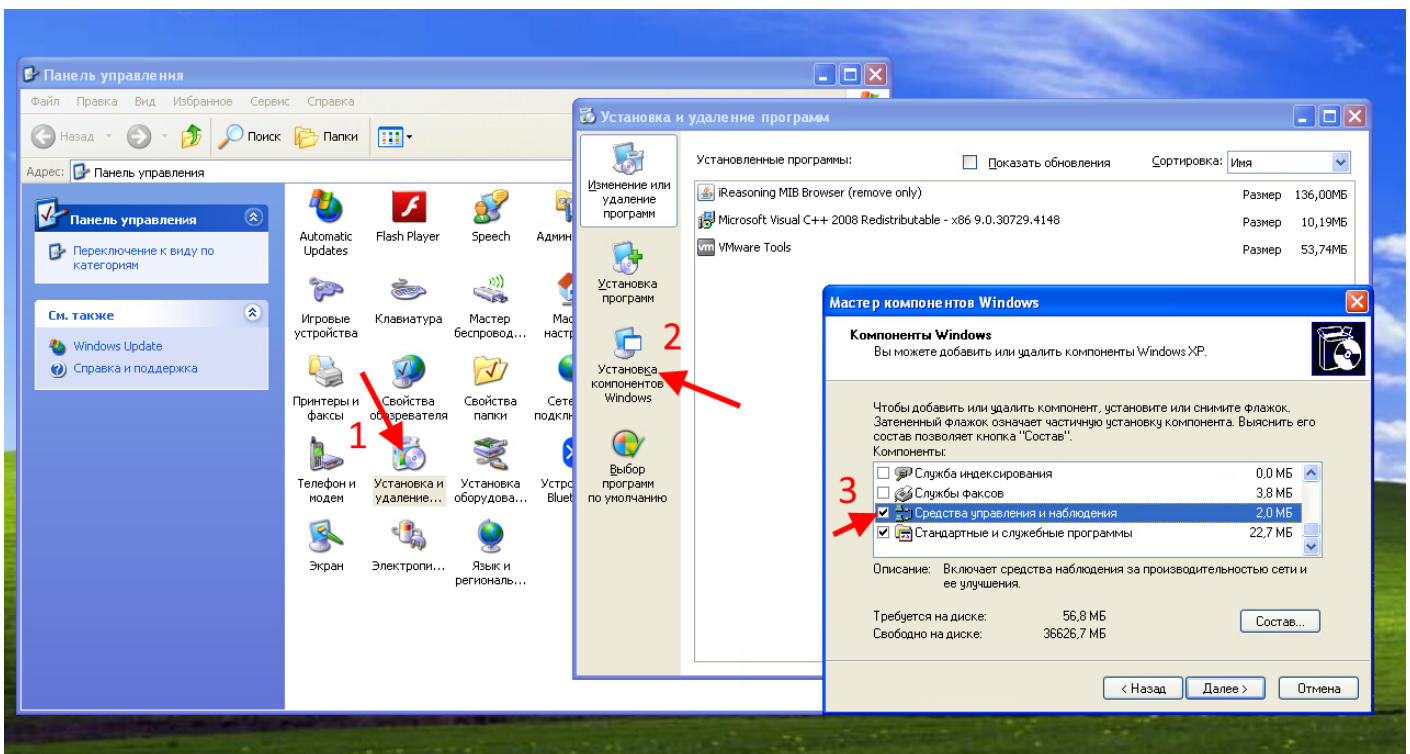
Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

Официальная документация по данному разделу приведена в Онлайн-справке на продукт: <https://support.kaspersky.com/help/KUMA/3.0.3/ru-RU/239864.htm>

?????????? ?? ??????? Windows.

?????????? ??????? SNMP

В статье рассматривается настройка на ОС Windows XP. Перейдите в **Панель управления - Установка и удаление программ - Установка компонентов Windows**. Установите Средства управления и наблюдения и провайдер WMI SNMP (если есть).

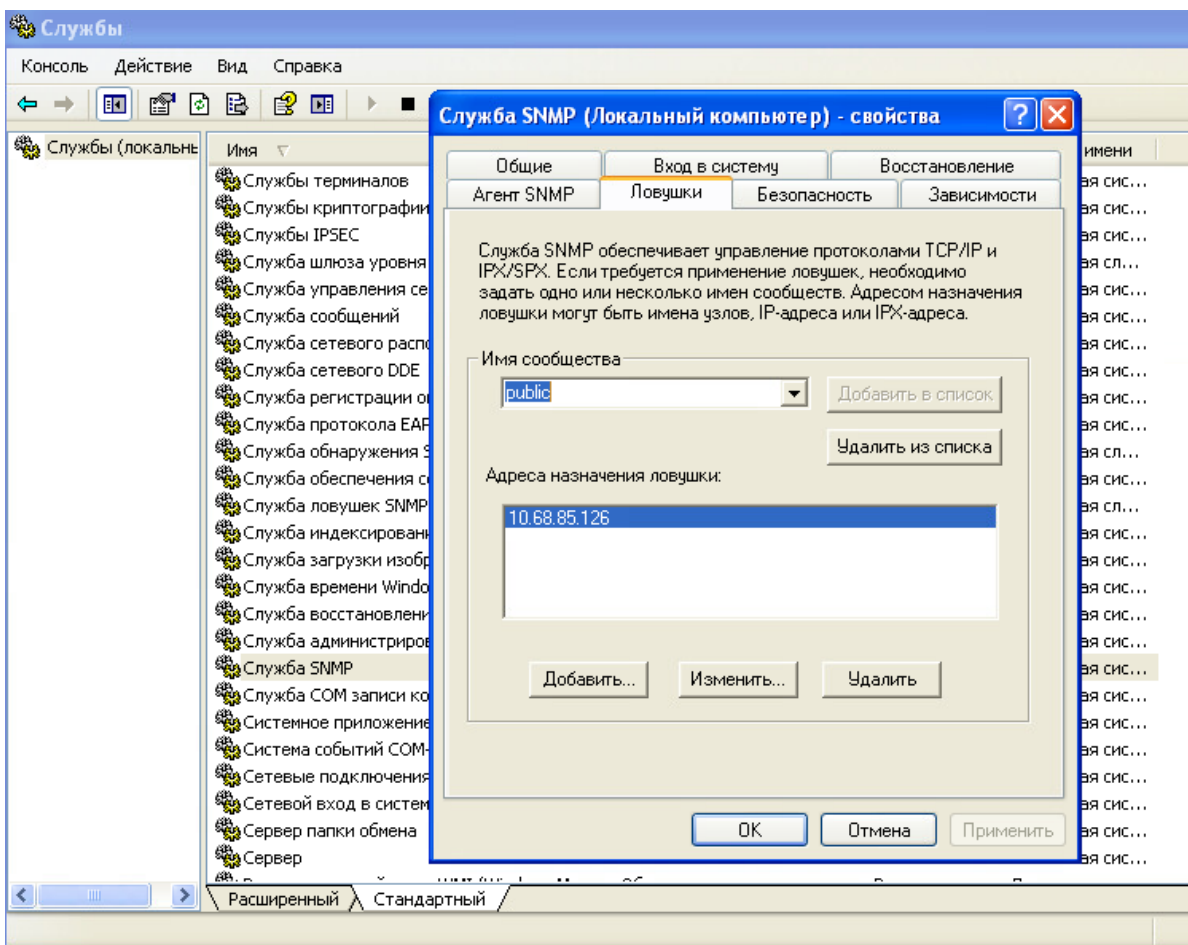


Дождитесь завершения установки и перезагрузите компьютер.

Убедитесь, что службы SNMP запущена (**Панель управления - Администрирование - Службы**): Служба SNMP (SNMP Service) и Служба ловушек SNMP (SNMP Trap). Если какие-то из перечисленных ниже служб не запущены - Запустите

# ?????????? ???????? SNMP

Перейдите в **Панель управления - Администрирование - Службы - Служба SNMP (Свойства) - Вкладка Ловушки**

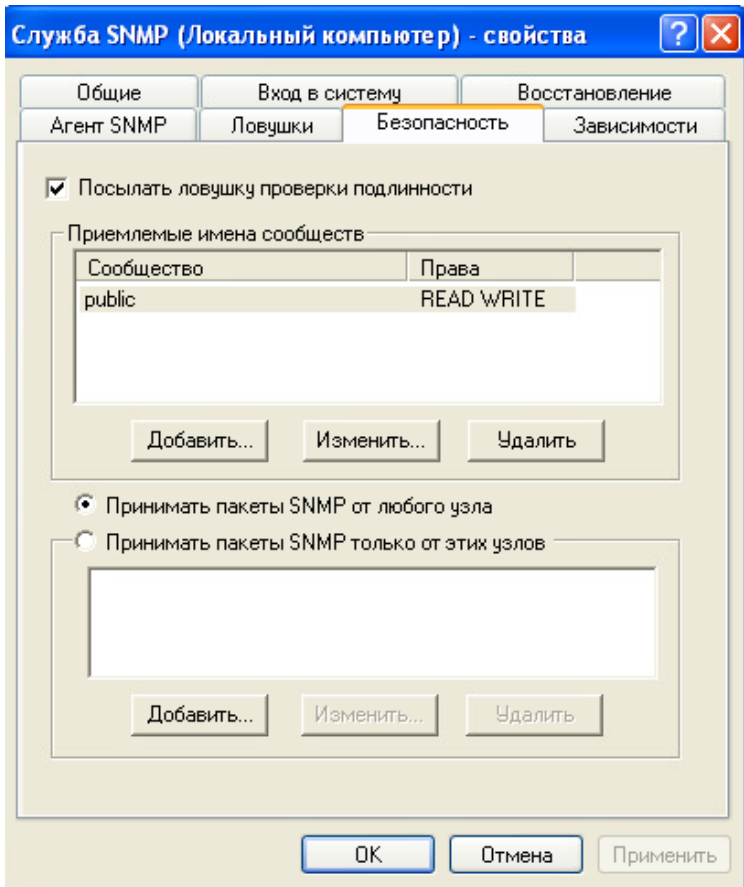


Добавьте имя сообщества: **public**

Адрес назначения ловушек: **<IP\_адрес\_коллектора>**

На вкладке Безопасность:

- Установите флажок: Посылать ловушку проверки подлинности (Send authentication trap)
- В таблице Приемлемые имена сообществ (Accepted community names) добавьте сообщество: public, с правами READ WRITE
- Установите флажок: Принимать пакеты SNMP от любого узла (Accept SNMP packets from any hosts)



Затем Применить и ОК.

?????????? ?? ?????????? KUMA

Создайте коллектор со следующим транспортом:

## Редактирование коллектора

Подключение источников

**Транспорт**

Подключите источник, от которого хотите получать события. Подробнее см. [в онлайн-справке](#).

Основные параметры    Дополнительные параметры

Коннектор

Тип\* ⓘ  ← 1

**SNMP-ресурс**

Версия SNMP\*  ← 2

URL\* ⓘ  ← 3

+ SNMP-ресурс

**Параметры**

Поступающие по SNMP данные необходимо нормализовать, связав OID объекта из события с Ключом и указав название нормализуемого параметра. На этапе парсинга событий в коллекторе значение из поля Ключ будет использоваться при сопоставлении полученных данных с полями KUMA.

+ Добавить    Удалить    Очистить значения    Применить значения OID для WinEventLog ← 4

<input type="checkbox"/> Название параметра	OID	Ключ
---	-----	------

В дополнительных параметрах в случае Русской локали в ОСкажите явно кодировку:

## Редактирование коллектора

Подключение источников

**Транспорт**

Подключите источник, от которого хотите получать события. Подробнее см. [в онлайн-справке](#).

Основные параметры    Дополнительные параметры

Отладка

Кодировка символов ⓘ  ← 1

В качестве парсера рекомендуем использовать комьюнити нормализатор (предварительно импортируйте его в KUMA, пароль импорта: `q123123Q!`): [ссылка](#)

Задайте маршрут куда отправлять обработанные события коллектором:

Подключение источников

Транспорт

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий

**Маршрутизация**

Проверка параметров

### Маршрутизация

Укажите, куда следует отправлять полученные события. Подробнее см

+ Добавить    Удалить

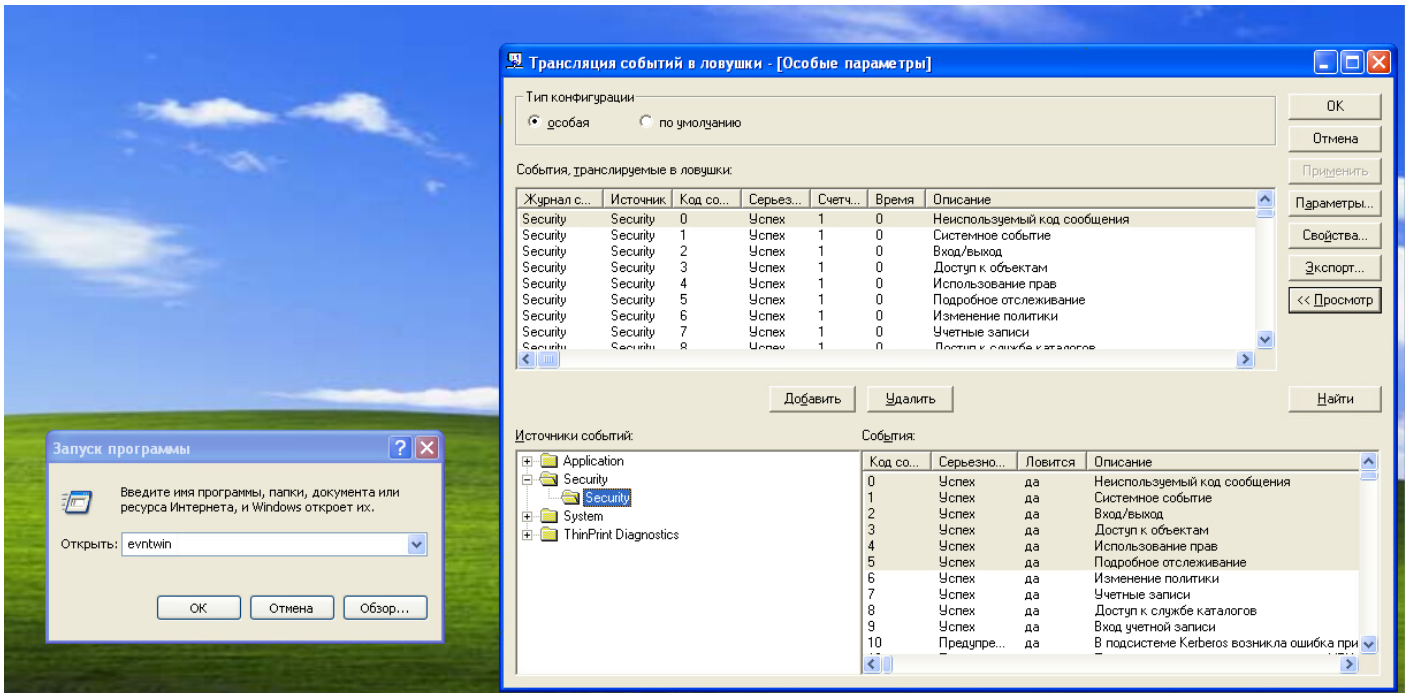
<input type="checkbox"/>	Название	Тип
<input type="checkbox"/>	[OOTB] Storage	storage
<input type="checkbox"/>	[OOTB] Correlator	correlator

Нажмите сохранить и создать сервис, скопируйте строку установки и выполните ее в консоли SSH.

SNMP использует порт **161 UDP** для общих сообщений, для ловушек используется порт **162 UDP**. Для прослушки порта SNMP обновите параметры службы в Linux (предварительно скопируйте ID коллектора), инструкция как настроить прослушку ниже 1024 порта в Linux: [ссылка](#)

# ?????????? ??????? ?? ?????????? Windows

Нажмите **Пуск - Выполнить** - Введите: **eventwin**



- В переключателе Тип конфигурации (Configuration type) выберите особая (Custom), а затем нажмите на кнопку Правка (Edit)
- В блоке параметров Источники событий (Event sources) найдите и добавьте с помощью кнопки Добавить (Add) события, которые вы хотите отправить в коллектор KUMA с установленным коннектором SNMP Trap (рекомендуется отправлять все из папки Security)
- Нажмите на кнопку Settings, в открывшемся окне установите флажок Не применять глушитель (Don't apply throttle) и нажмите OK
- Нажмите Применить (Apply) и OK

## ?????????? ?????????? ?????????? ?? Windows

Создайте и удалите тестового пользователя в системе для генерации событий в **Панель управления - Администрирование - Управление компьютером - Локальные пользователи - Папка пользователи**.

При корректных настройках в кума должно отобразиться событие:

SELECT ** FROM events WHERE ServiceID = '8f25c83f-2ee2-46b0-a81f-3aaf495feb72' ORDER BY Timestamp DESC LIMIT 250							Счетчик ограниченного SID: 0	
TenantID	Raw	DeviceEventClassID	Timestamp ↓	DeviceHostName	Type	DestinationUserN	DeviceAddress	10.68.85.137
Main	[*agentAddrSNMPHea...	560	17.04.2024 10:49:05	WINXP-PC	Base		DeviceAssetID	<a href="#">WINXP-PC</a>
Main	[*agentAddrSNMPHea...	562	17.04.2024 10:49:05	WINXP-PC	Base		DeviceEventCategory	3
Main	[*agentAddrSNMPHea...	560	17.04.2024 10:48:57	WINXP-PC	Base		DeviceEventClassID	560
Main	[*agentAddrSNMPHea...	562	17.04.2024 10:48:57	WINXP-PC	Base		DeviceHostName	WINXP-PC
Main	[*agentAddrSNMPHea...	562	17.04.2024 10:46:59	WINXP-PC	Base		DeviceNtDomain	WORKGROUP
Main	[*agentAddrSNMPHea...	560	17.04.2024 10:46:59	WINXP-PC	Base		DeviceProduct	Windows
Main	[*agentAddrSNMPHea...	562	17.04.2024 10:46:59	WINXP-PC	Base		DeviceReceiptTime	17.04.2024 10:50:38.987
Main	[*agentAddrSNMPHea...	560	17.04.2024 10:46:59	WINXP-PC	Base		DeviceTimeZone	+03:00
Main	[*agentAddrSNMPHea...	564	17.04.2024 10:46:59	WINXP-PC	Base		DeviceVendor	Microsoft
Main	[*agentAddrSNMPHea...	562	17.04.2024 10:46:54	WINXP-PC	Base		SourceNtDomain	WINXP-PC
Main	[*agentAddrSNMPHea...	562	17.04.2024 10:46:54	WINXP-PC	Base		SourceProcessName	SAM_USER
Main	[*agentAddrSNMPHea...	564	17.04.2024 10:46:54	WINXP-PC	Base		SourceUserID	Administrator
Main	[*agentAddrSNMPHea...	562	17.04.2024 10:46:54	WINXP-PC	Base		SourceUserName	WINXP-PC\$
Main	[*agentAddrSNMPHea...	564	17.04.2024 10:46:54	WINXP-PC	Base		DeviceCustomString1	READ_CONTROL,WRITE_DAC,WritePreferences,ReadAccount,WriteAccount,Задание пароля (без знания старого пароля),ListGroups
Main	[*agentAddrSNMPHea...	560	17.04.2024 10:46:54	WINXP-PC	Base		DeviceCustomString1Label	Доступ
Main	[*agentAddrSNMPHea...	560	17.04.2024 10:46:54	WINXP-PC	Base		DeviceCustomString2	DOMAINS\Account\Users\00000400
Main	[*agentAddrSNMPHea...	564	17.04.2024 10:46:46	WINXP-PC	Base		DeviceCustomString2Label	Имя объекта
Main	[*agentAddrSNMPHea...	562	17.04.2024 10:46:46	WINXP-PC	Base		Service	<a href="#">WinXp SNMP</a>
Main	[*agentAddrSNMPHea...	562	17.04.2024 10:46:46	WINXP-PC	Base		FileName	C:\WINDOWS\system32\lsass.exe

Revision #4

Created 2024-04-17 07:43:33 UTC by Boris RZR

Updated 2024-12-18 10:16:19 UTC by Koala