Инвентаризация

Инвентаризация

Вернуться в оглавление Документации Pandora FMS

Инвентаризация

Введение

Enterprise версия Pandora FMS позволяет вести инвентаризацию устройств, контролируемых Pandora FMS. С помощью такой инвентаризации можно вести список процессоров, карт, оперативной памяти, патчей, программного обеспечения и т.д. серверов компании.

Инвентаризация не зависит от мониторинга и может быть получена локально (через программные агенты Pandora FMS) или удаленно:

- Модель и скорость процессора (MS Windows®, GNU/Linux®).
- Хранилище и файловые системы.
- Версия прошивки (сетевое оборудование).
- Конфигурация устройства (сетевое оборудование).
- Серийные номера и лицензии (например: MS Office®, MS Windows®).
- Установленные на компьютере приложения (MS Windows®, Android Linux®, GNU/Linux®).
- Сетевые карты и их MAC-адреса, связанные с IP-адресами.
- Модули памяти RAM и их объем (MS Windows®, GNU/Linux®).
- Рут установлены.
- Запуск сервисов.
- Устройства хранения (MS Windows®, GNU/Linux®).
- Системные пользователи.

Сбор данных для инвентаризации

Сбор данных для инвентаризации систем осуществляется двумя способами:

Удаленно, с помощью модулей инвентаризации, через *скрипты* интегрированные в Pandora FMS, которые выполняют *queries* WMI , или *скрипты*, выполняемые через SSH с помощью Expect или аналогично.

На местном уровне, с помощью программного агента Pandora FMS, через *плагины* в агенте.

Модули инвентаризации

Модули инвентаризации - это удаленные модули, которые выполняют команду на удаленной машине. Эти модули работают аналогично *плагину*. Те же модули могут быть определены как «локальные», если они получают данные через агента.

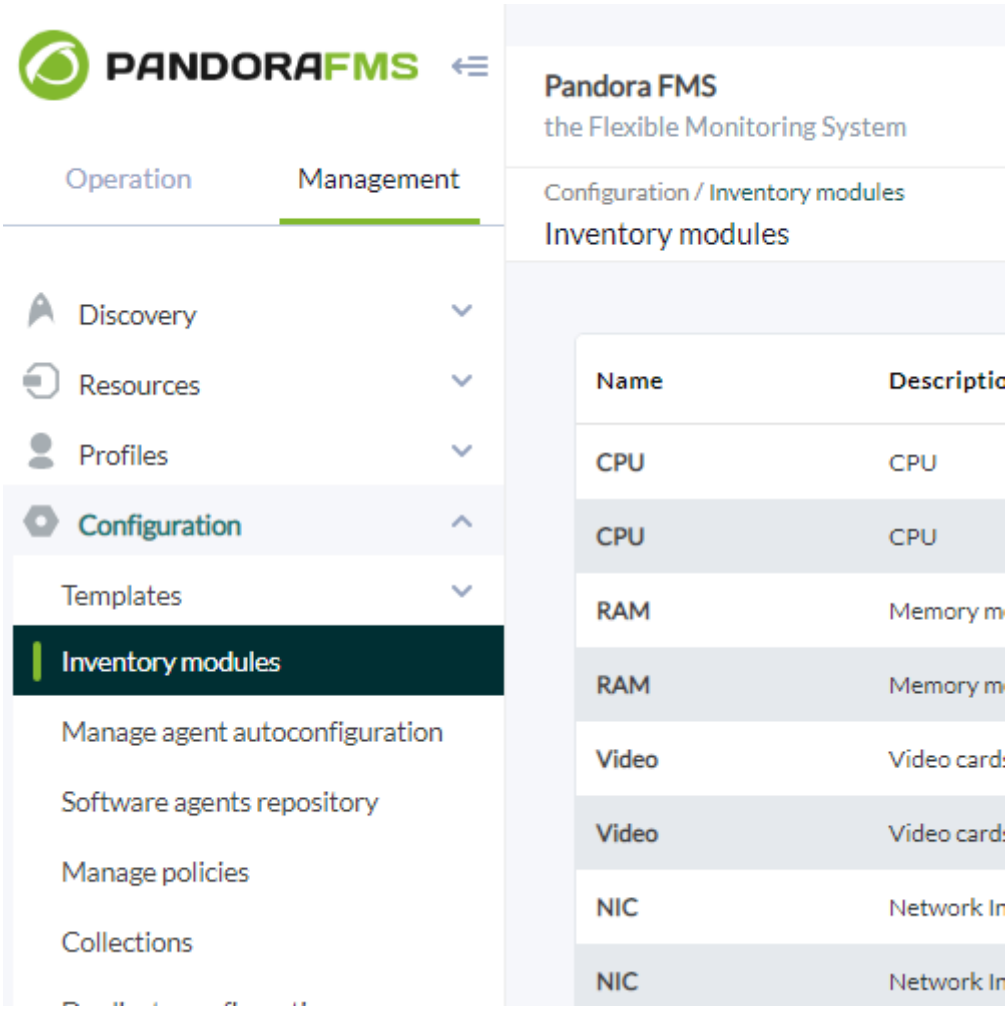
В параметрах пользователя и пароля можно использовать следующие макросы: _agentcustomfield_n_ (Пользовательское поле номера агента).

Удаленная инвентаризация

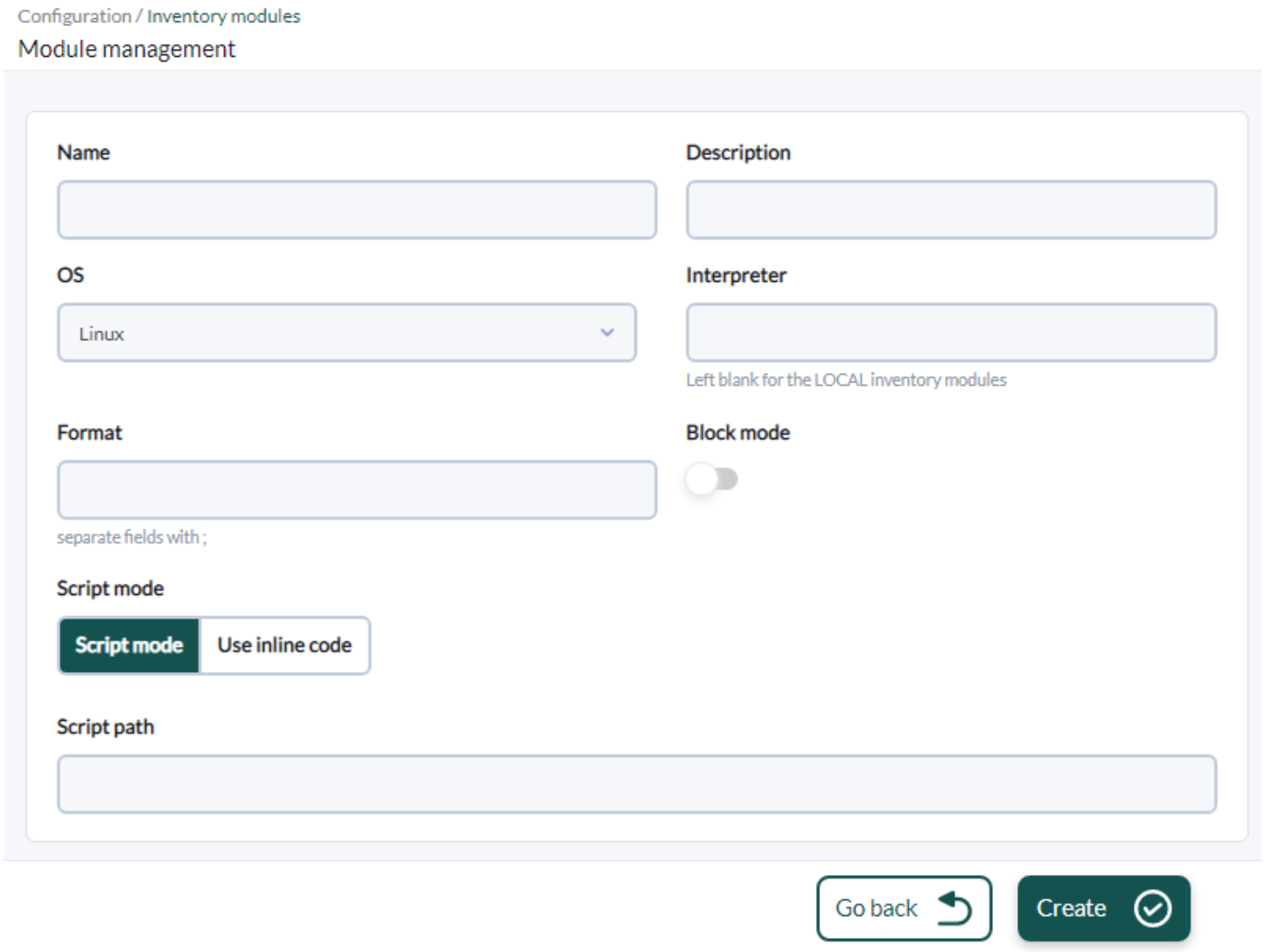
Создание удаленных модулей

Создание администратором модуля удаленной инвентаризации не является обычным делом; они уже поставляются с предустановленным Pandora FMS Enterprise. Однако Pandora FMS позволяет создавать собственные модули инвентаризации или изменять существующие с помощью редактора модулей инвентаризации.

Чтобы создать удаленный модуль, перейдите в раздел Configuration → Inventory Modules, где перечислены все созданные модули инвентаризации.



Чтобы создать новый модуль, нажмите на Create.



OS: Выберите целевую операционную систему для модуля.

Interpreter: *Оставьте пустым, если это локальный модуль.* Поле, в которое помещается командный интерпретатор, используемый в модуле. Это может быть Shell Script, Perl или другой допустимый интерпретатор для сервера инвентаризации, работающего в системе Linux.

Block mode: Отображает и обнаруживает изменения в конфигурации.

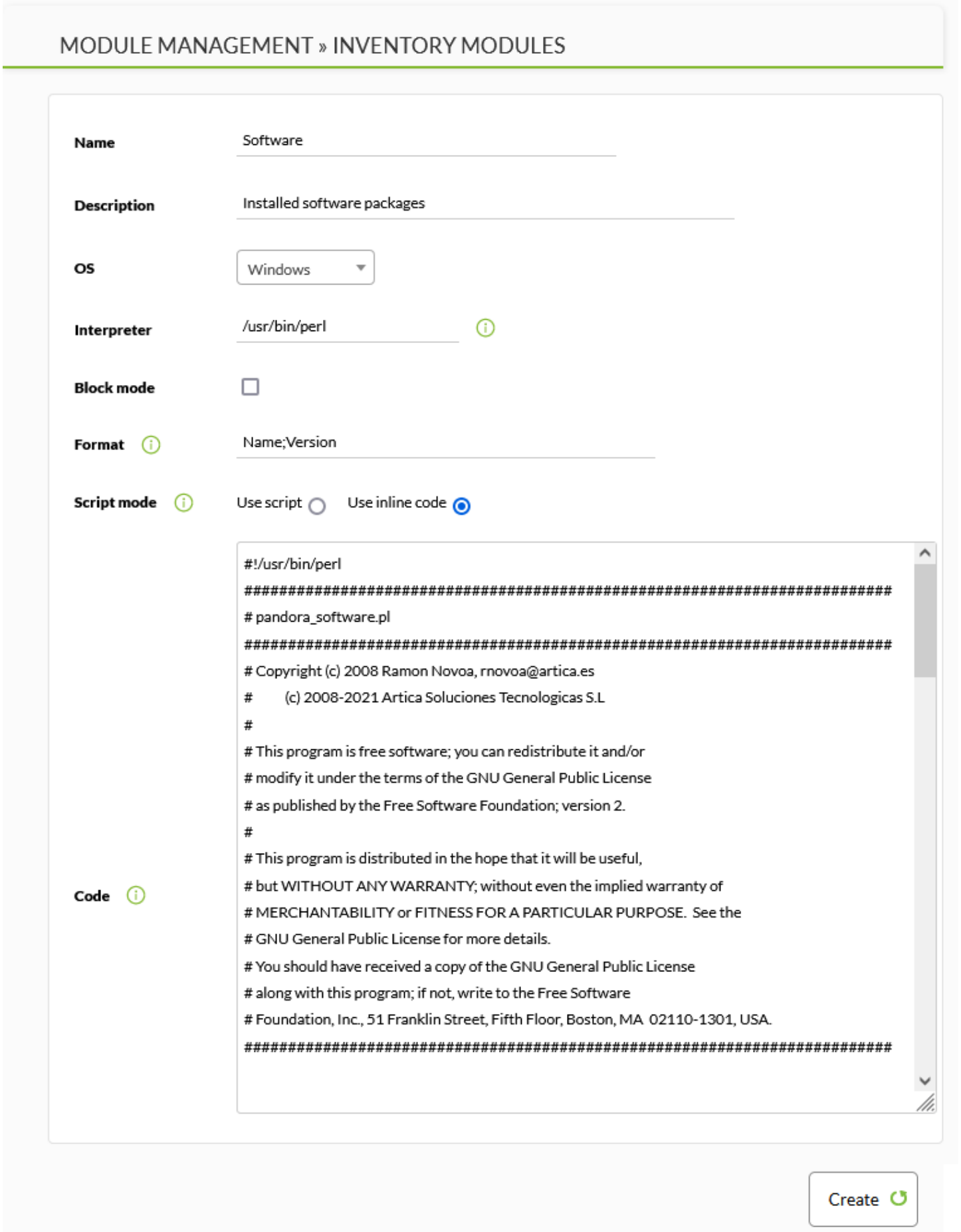
Format: Введите поля, разделенные ；, которые будут возвращены модулем.

Code: *Оставьте пустым, если это локальный модуль.* Код модуля; обычно это код Perl или Shell Script. Если бы это был двоичный код, то ему потребовалась бы другая процедура загрузки, вводимая вспомогательными *скриптами*.

Очень важно правильно выбрать операционную систему, так как при добавлении дополнительных модулей инвентаризации в агенте появятся только те модули, операционная система которых соответствует

операционной системе модуля и операционной системе агента.

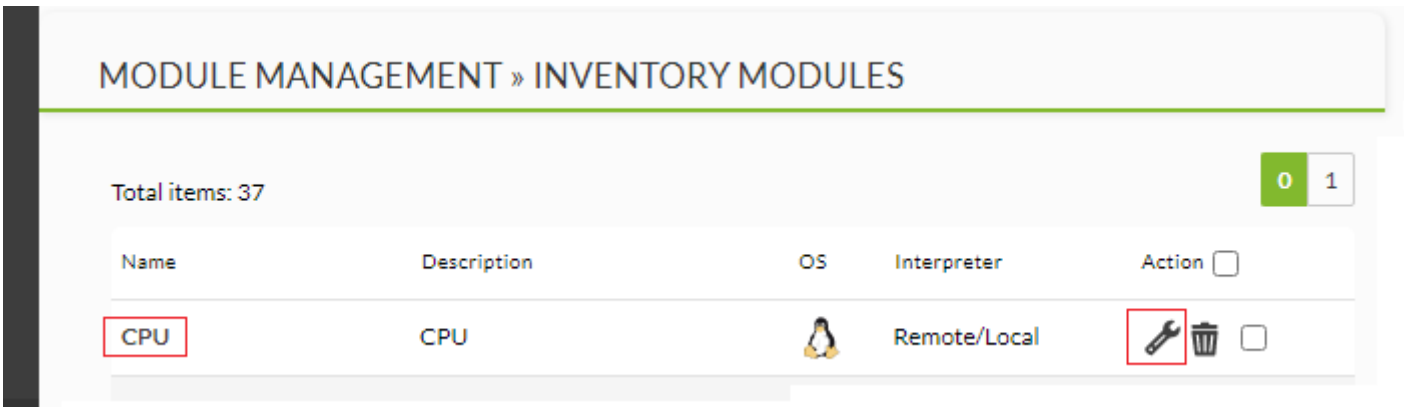
После создания модуля нажмите кнопку Create:



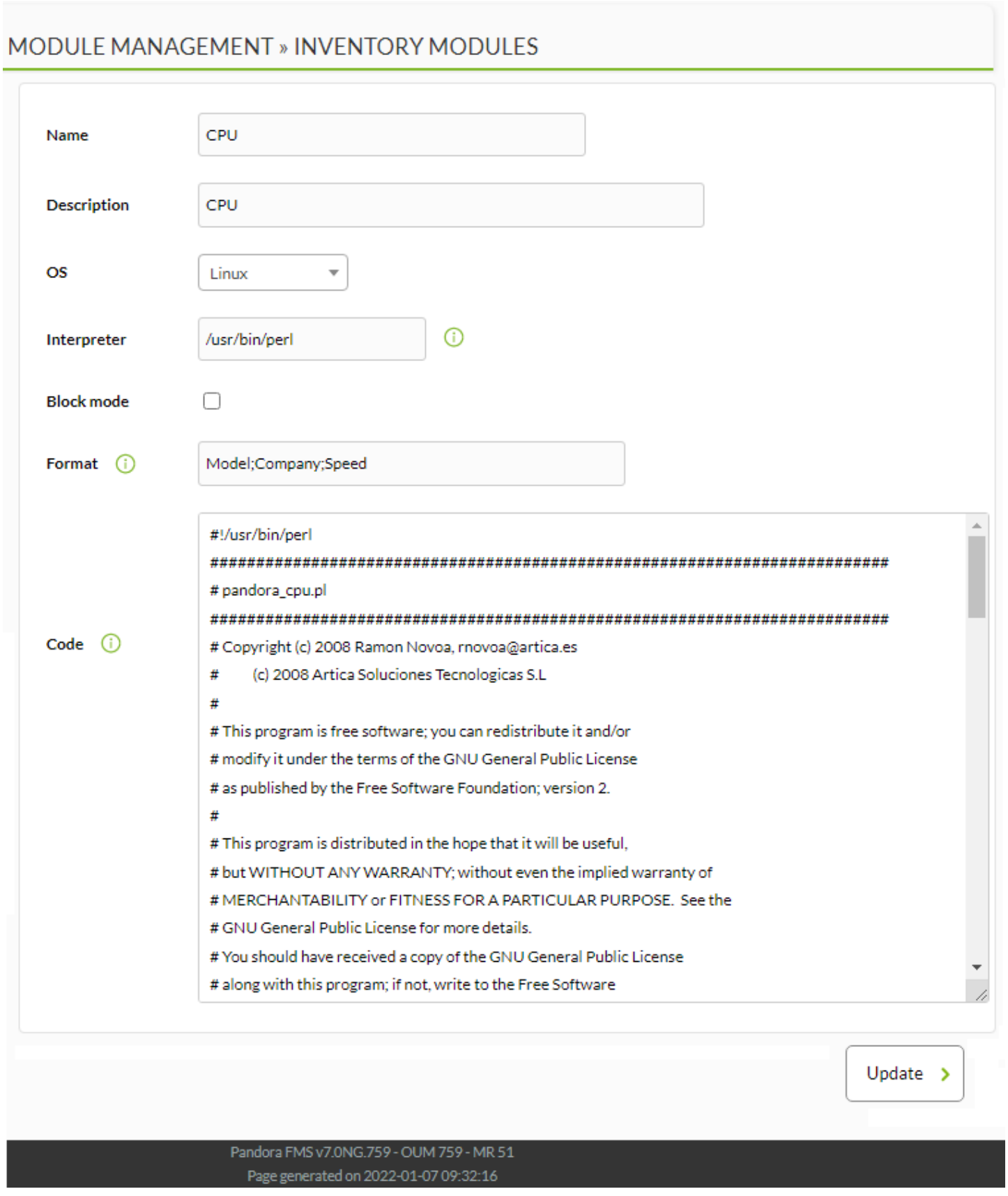
редактирование удаленных модуля

Чтобы отредактировать удаленный модуль, перейдите в Configuration → Inventory Modules,

где перечислены все созданные модули инвентаризации. Нажмите на в названии модуль, который вы хотите отредактировать, или на иконку ключа в колонке Action.



Снова появится страница создания модуля.

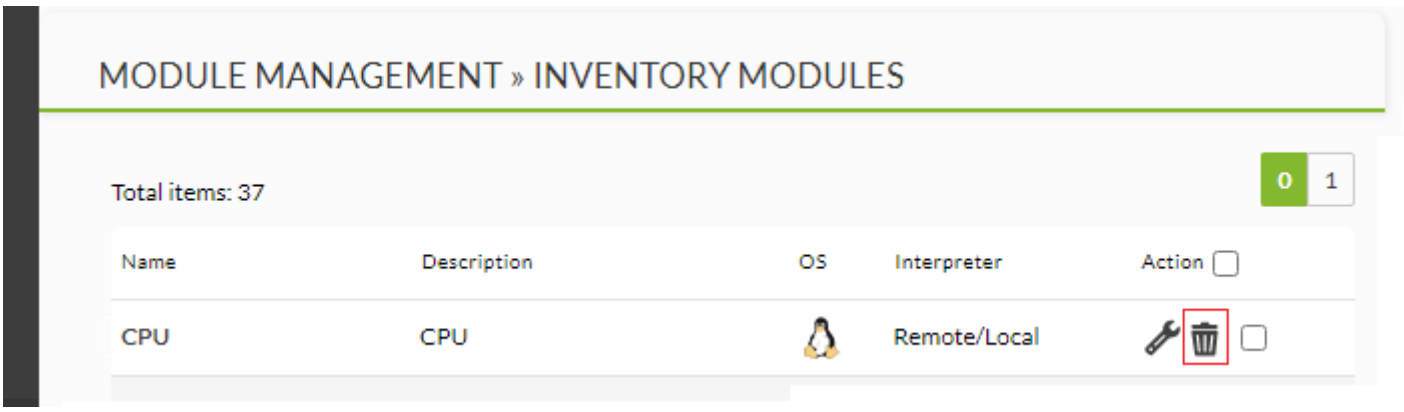


Измените нужные поля и нажмите на кнопку. Update.

Уничтожение удаленных модулей

Чтобы удалить удаленный модуль, перейдите в раздел Configuration → Inventory Modules,

где перечислены все созданные модули инвентаризации. Нажмите на значок корзины в столбце Action модуля, который необходимо удалить.

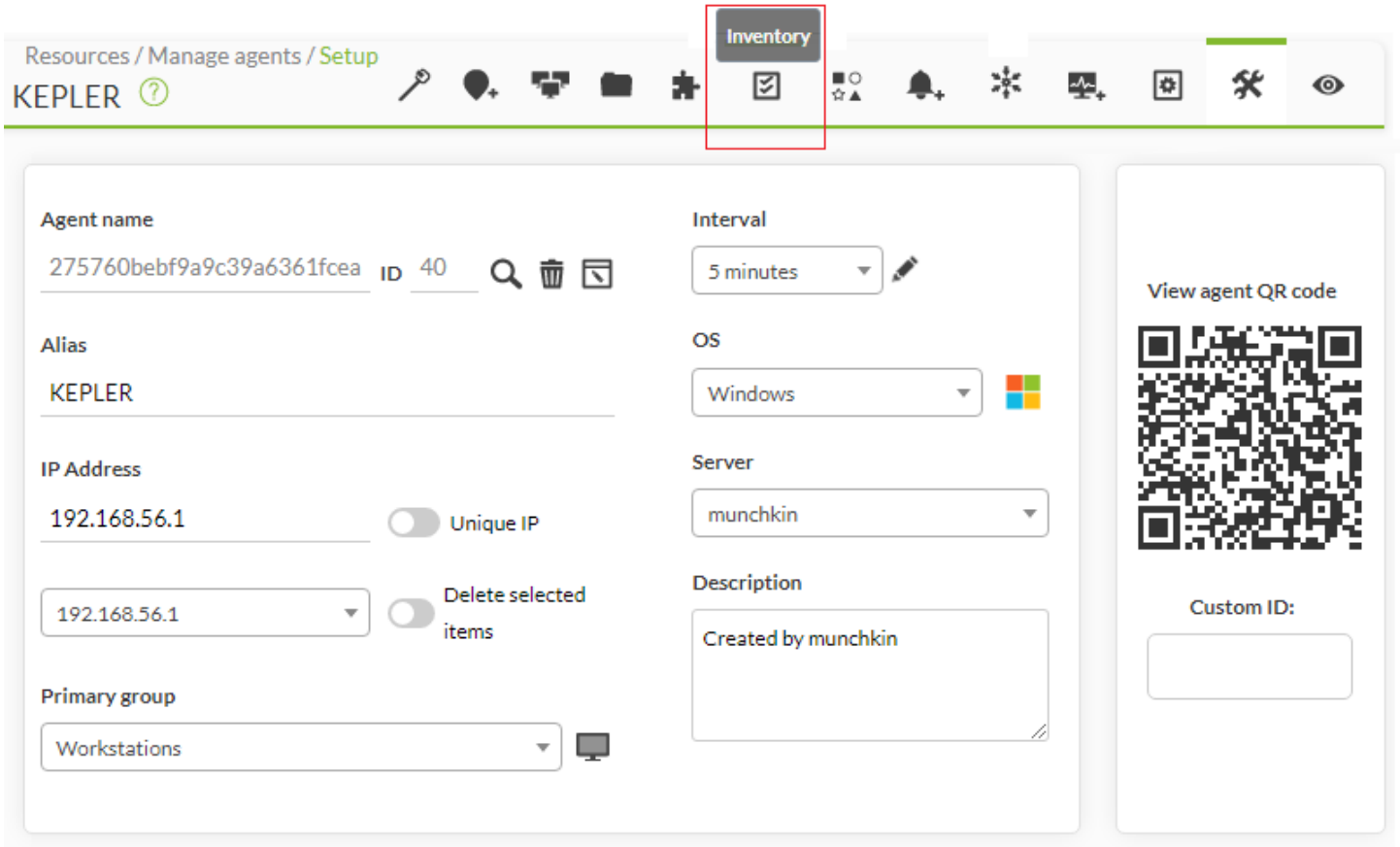


Кроме того, каждый из них имеет флажок, который позволяет выбирать их пакетно, а не удалять по одному.

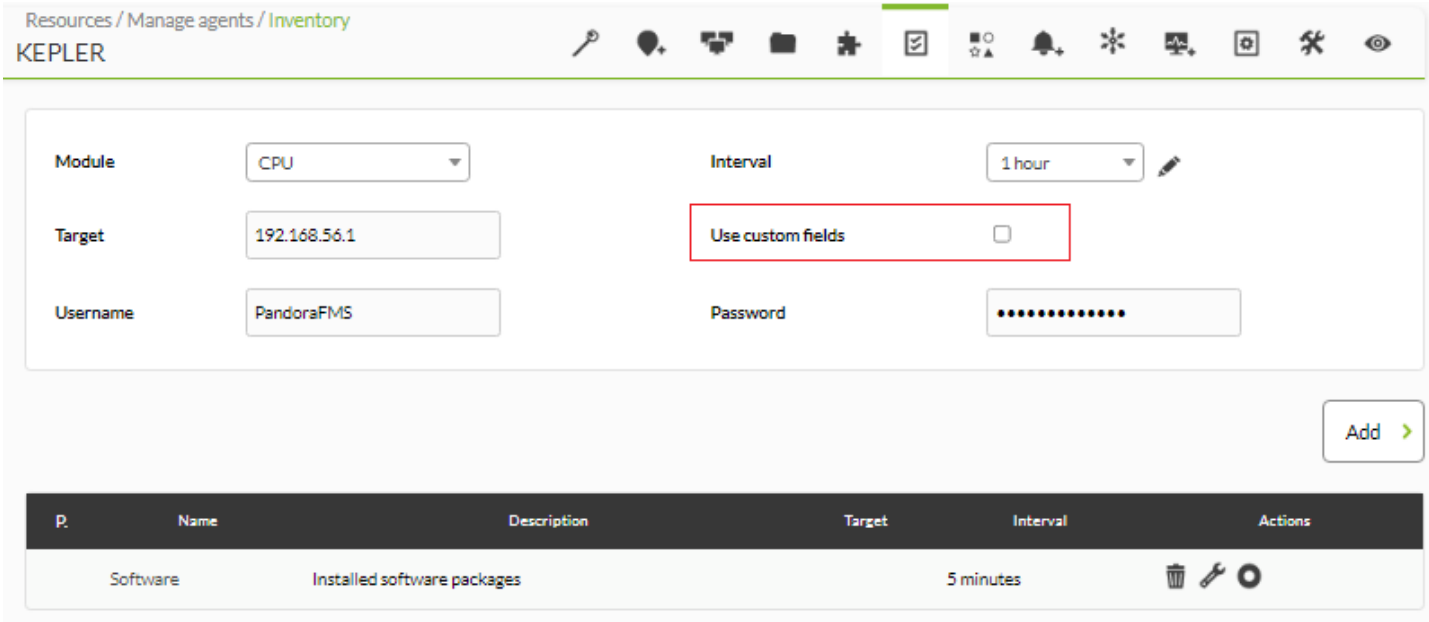
Назначение удаленных модулей

Назначение модулей инвентаризации осуществляется в самом агенте, на вкладке администрирования агента.

Вы должны нажать на вкладку Inventory.



Откроется страница, на которой можно добавить модули инвентаризации.



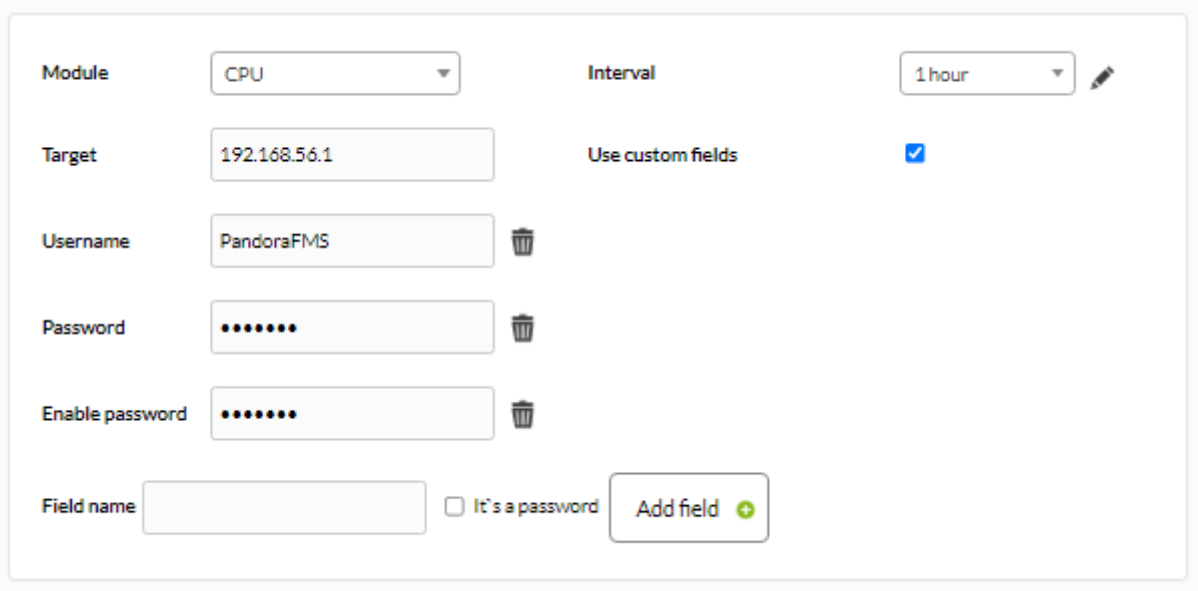
- Module: Выберите модуль инвентаризации, который необходимо добавить. Будут отображаться только те модули, операционная система которых совпадает с операционной системой агента.
- Target: IP-адрес или имя сервера, с которого вы хотите произвести инвентаризацию.
- Interval: Выберите интервал времени, через который запускается модуль инвентаризации.
- Username: Пользователь, который будет использоваться для запуска модуля инвентаризации.
- Password: Пароль пользователя, который будет использоваться для запуска модуля инвентаризации.

Начиная с версии v7.0NG.724, можно определять поля вместо обычных полей пользователя и пароля. Для этого необходимо активировать следующий флажок:

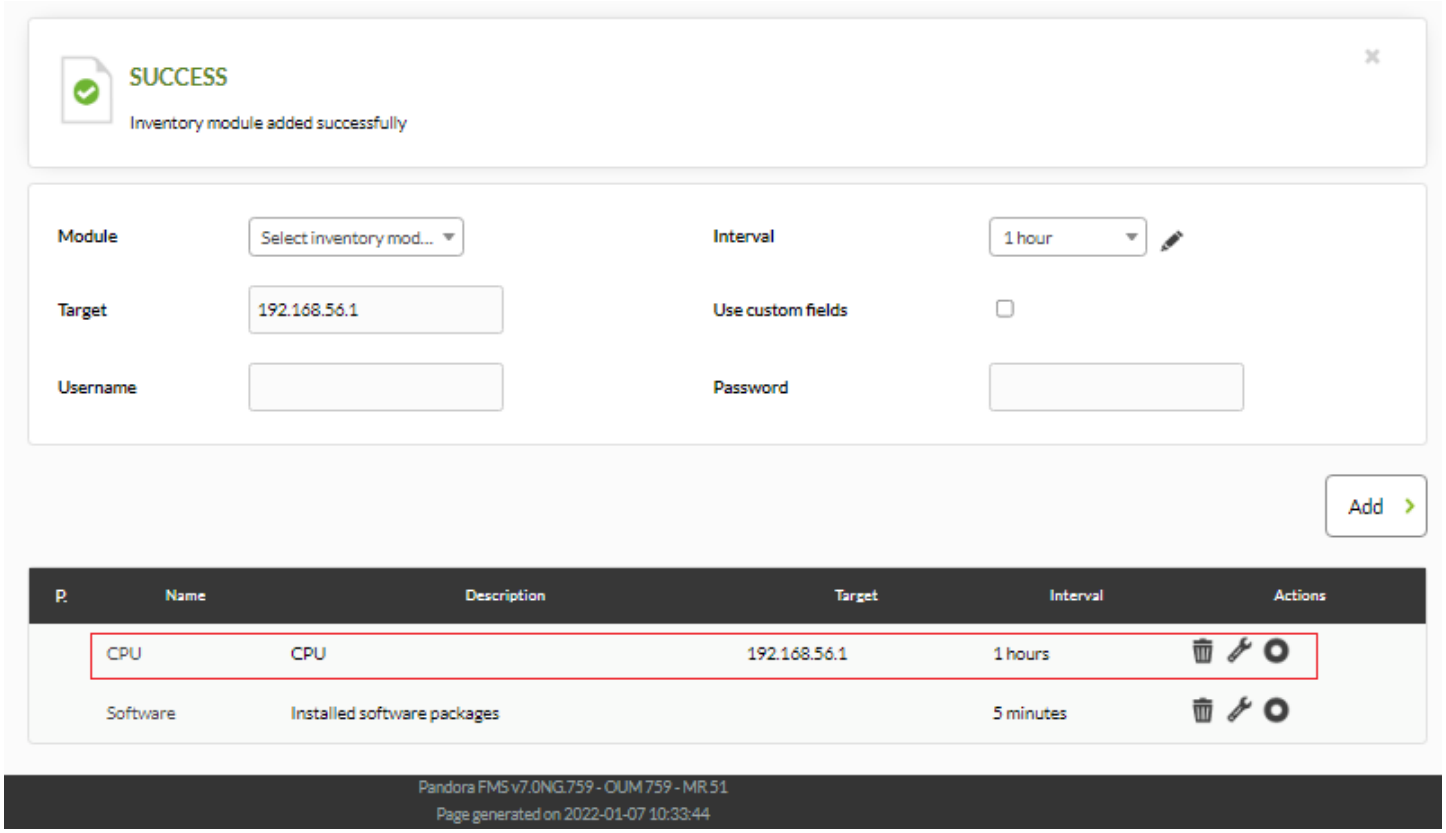
После этого появится элемент управления для добавления новых полей (Add field):

В этом элементе управления введите нужное имя перед его добавлением. Если вы укажете, что поле должно содержать пароль, значение будет храниться в базе данных в сокрытом виде.

После создания полей мы можем присвоить им значение и, наконец, добавить модуль. Эти поля должны применяться в порядке создания при выполнении *скрипта* удаленной инвентаризации.



После заполнения формы нажмите кнопку Add. Модуль будет добавлен в модули инвентаризации.



Редактирование назначенного модуля удаленной инвентаризации

Модули инвентаризации можно редактировать; это редактирование осуществляется на той же странице, где они были созданы.

Чтобы отредактировать модуль инвентаризации, нажмите на название модуля или на значок ключа, показанный на рисунке.

Удаление назначенного удаленного модуля инвентаризации

Можно удалять модули инвентаризации; удаление производится на той же странице, где они были созданы.

Чтобы удалить модуль инвентаризации, нажмите на значок корзины в колонке Action модуля.

Полный пример процесса создания удаленного модуля инвентаризации

Предположим, вам нужно получить список физических адресов адаптера с сервера, в данном случае сервера Unix. Эту информацию обычно получают с помощью команды `arp -a -n`, которая при запуске на сервере будет выглядеть примерно так:

```
artica@galaga:~$ arp -a -n
? (192.168.70.74) at 08:00:27:39:BF:6F [ether] on eth2
? (192.168.70.162) at B4:74:9F:94:98:84 [ether] on eth2
? (192.168.50.30) at 08:00:27:10:D1:1A [ether] on eth0
? (192.168.70.90) at 98:0C:82:54:2F:DE [ether] on eth2
? (192.168.50.2) at 08:00:27:EA:B2:FF [ether] on eth0
? (192.168.70.135) at C8:60:00:4B:96:67 [ether] on eth2
? (192.168.60.182) at FE:26:C5:91:B1:DA [ether] on tap0
```

В данном примере мы ищем IP-адрес, MAC-адрес и имя адаптера.

В Shellscript это можно сделать следующим образом, используя «» для разделения полей:

```
arp -a -n | sort | grep -v incomplete | awk '{ print $2,$4,$7 }'
```

Это то, что необходимо для «импорта» этой информации в сервер удаленной инвентаризации Pandora FMS. Для этого возьмите за основу слегка модифицированный модуль удаленной инвентаризации «CPU». Этот *скрипт* подключается через SSH к целевому

серверу и выполняет команду. Вывод команды должен возвращать каждое поле, разделенное символом `;` .

На этом этапе вам необходимо иметь навыки программирования, чтобы разработать или изменить *скрипты*. *Скрипты* удаленной инвентаризациии , хотя и не сложные, требуют определенных знаний Perl, Shellscript или другого интерпретируемого языка; они также могут быть выполнены на Java, C++, и вызывать их выполнение из модуля, при условии, что он возвращает значения каждого определенного поля, разделенные `;` и переходом строки для каждой единицы данных.

```
#!/usr/bin/perl
################################################################################
# pandora_linux_arptable.pl
################################################################################
# Copyright (c) 2012 Sancho Lerena <slerena@artica.es>
#           (c) 2012 Artica Soluciones Tecnologicas S.L
#
# This program is free software; you can redistribute it and/or
# modify it under the terms of the GNU General Public License
# as published by the Free Software Foundation; version 2.
#
# This program is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
# GNU General Public License for more details.
# You should have received a copy of the GNU General Public License
# along with this program; if not, write to the Free Software
# Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA  02110-1301,
USA.
################################################################################

use strict;
use warnings;

# Check for ssh
my $ssh_client = "ssh";
if (system("$ssh_client -v> /dev/null 2>&1")>> 8 != 255) {
    print "[error] $ssh_client not found.\n";
    exit 1;
}

if ($#ARGV <1) {
    print "Usage: $0 <target ip> <username>\n";
    exit 1;
}

my $target_ip = $ARGV[0];
my $username = $ARGV[1];
```

```
# Retrieve ARP table
my ($ip, $mac, $iface);
my $command = '/usr/sbin/arp -a -n | sort | grep -v incomplete | awk \'{ print
\$2,\$4,\$7 }\'';

my @info = `$ssh_client $username\@$target_ip "$command" 2> /dev/null`;
foreach my $line (@info) {
    if ($line =~ /^(.+)\s(.+)\s(.+)/) {
        $ip = $1;
        $mac = $2;
        $iface = $3;
        print "$ip;$mac;$iface\n";
    }
}

exit 0;
```

Чтобы SSH-соединение работало автоматически, необходимо скопировать открытый ключ пользователя root с сервера Pandora FMS на целевой сервер. Если целевое устройство имеет следующий IP-адрес, например, `192.168.50.10`, выполните следующие действия:

1. Создайте ключ на сервере Pandora FMS как корень. Заполните необходимые поля.

```
ssh-keygen
```

2. Используйте команду ssh-copy-id для копирования открытого ключа на целевой сервер (`192.168.50.10`) с целевым пользователем (в данном примере пользователем с именем artica):

```
ssh-copy-id -i /root/.ssh/id_rsa.pub artica@192.168.50.10
```

Вы должны ввести пароль пользователя artica один раз на 192.168.50.10, чтобы установить открытый ключ на целевом сервере.

3. Попробуйте подключиться; подключение произойдет без запроса пароля:

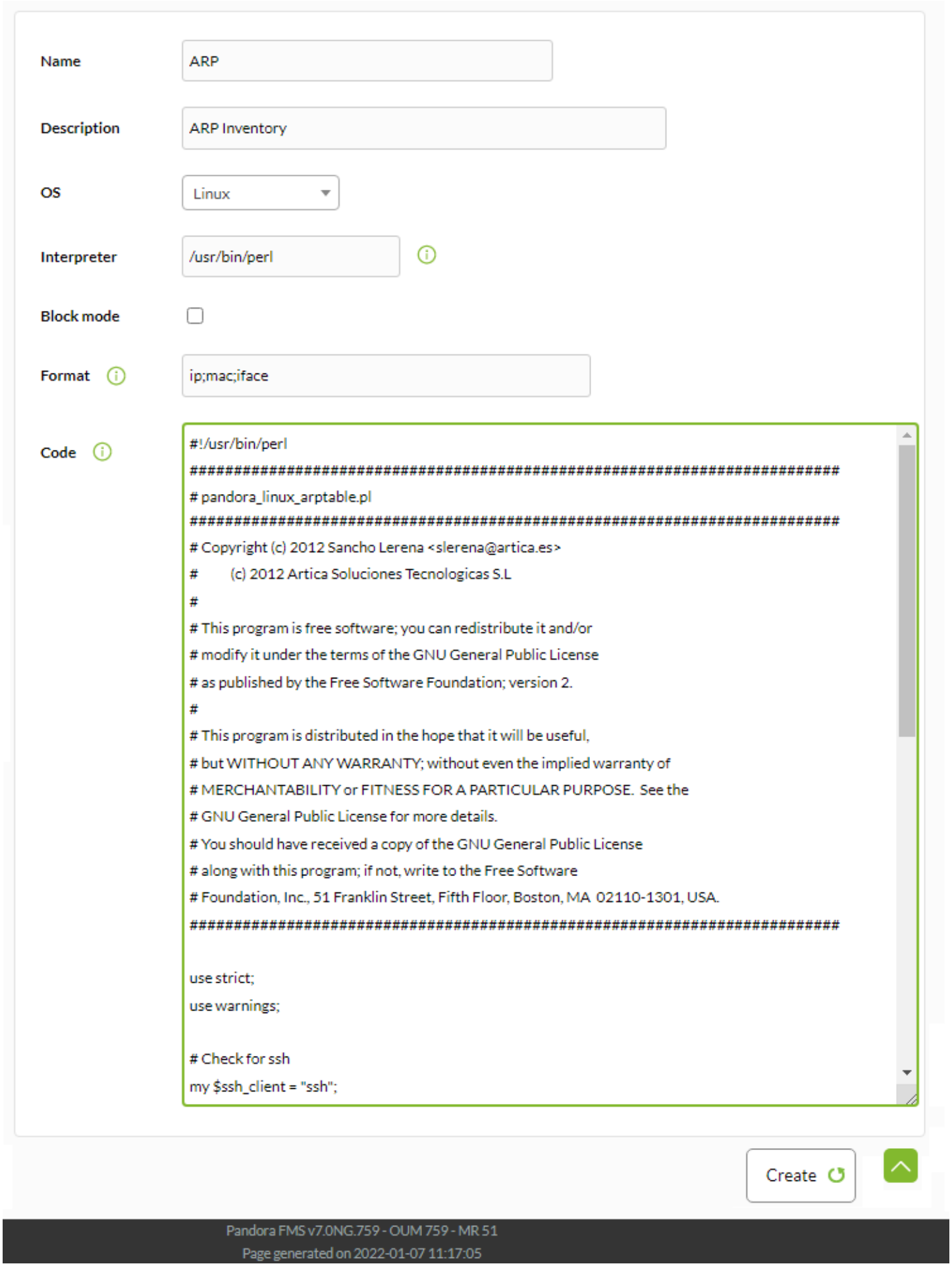
```
ssh artica@192.168.50.10
```

4. Если вы дошли до этого, тот же процесс будет выполняться и модулем инвентаризации, поэтому попробуйте запустить его из командной строки, сохранив предыдущий *скрипт* на диск (файл `temporal.pl`, т.е.) и запустить его с IP-адресом и пользователем как параметр:

```
perl temporal.pl 192.168.50.10 artica
(192.168.50.1);00:0f:ea:27:ba:f0;eth0
(192.168.50.3);08:00:27:98:f8:48;eth0
```

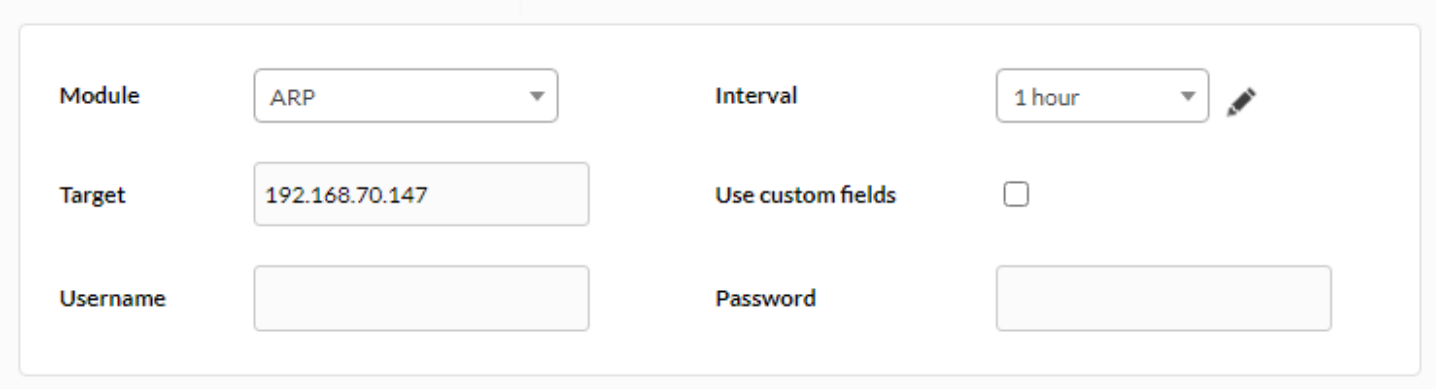
Обратите внимание, что *скрипт* удаленно вызывает `/usr/sbin/arp`. Команда должна

находиться в этом пути; если нет, переместите скрипт в другое место. Вы также можете заметить, что мы вызываем наш *скрипт* с помощью команды perl, которая обычно находится в `/usr/bin/perl`. Это то, что вы должны настроить при определении модуля, как показано ниже:

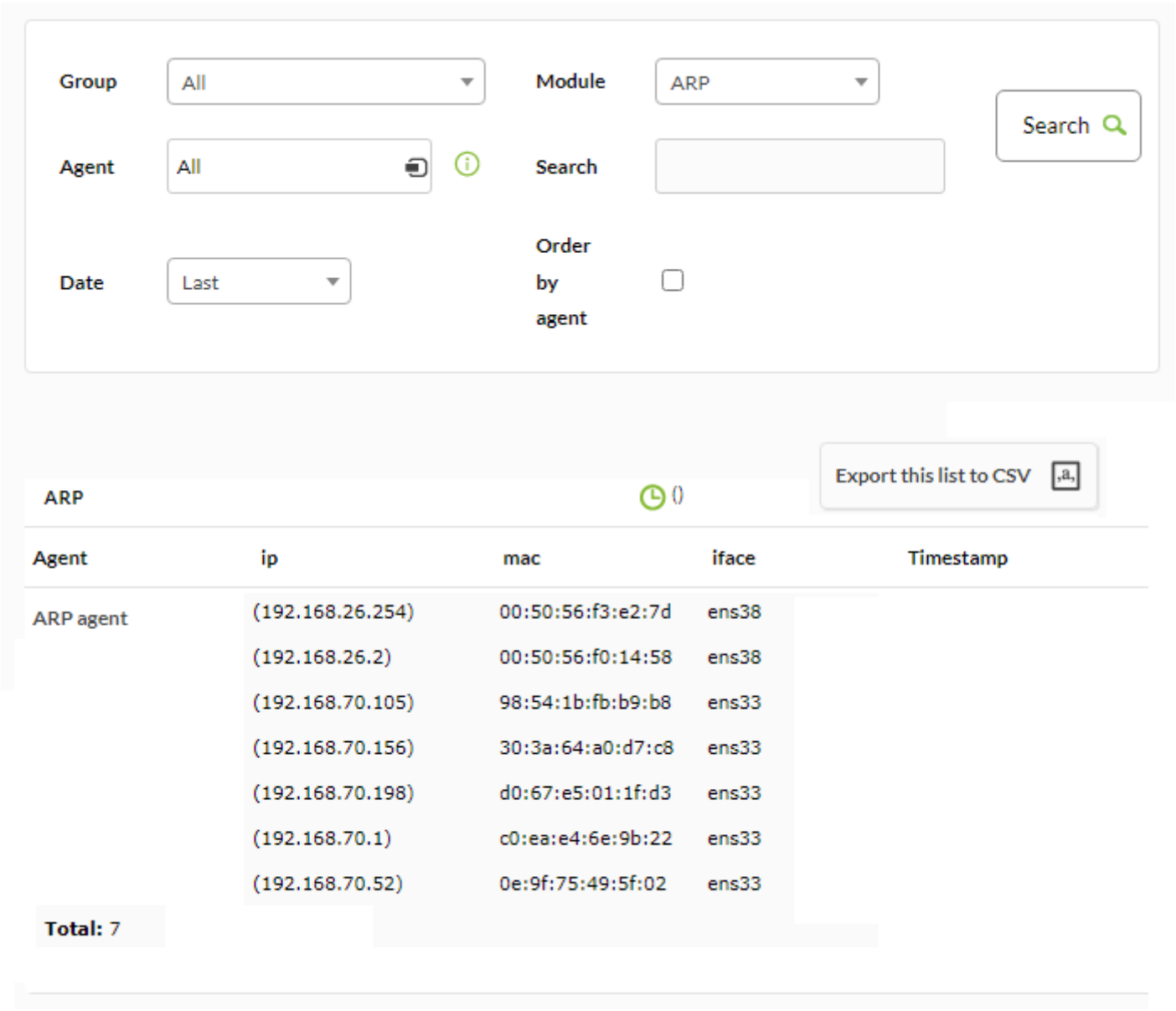


Применяя его к агенту, убедитесь, что операционная система совпадает. Если у вас разные операционные системы, вы должны создать отдельный модуль для каждой из них, потому

что один и тот же код не будет работать.



После выполнения этого модуля из консоли можно получить вид, подобный следующему:



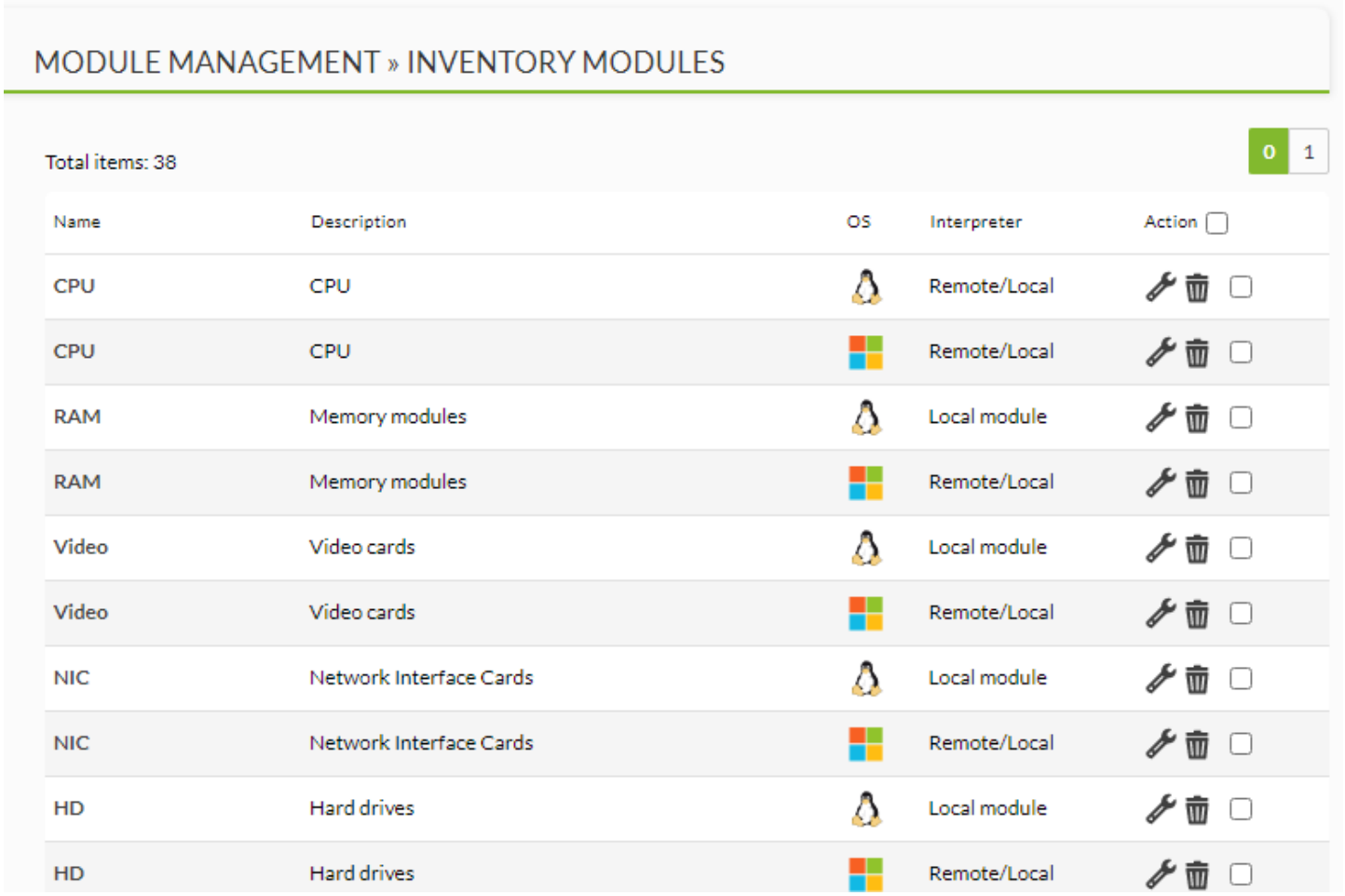
Локальная инвентаризация с помощью программных агентов

Mediante los C помощью программных агентов можно получить данные инвентаризации машины. Достаточно применить соответствующие модули инвентаризации в конфигурации программного агента.

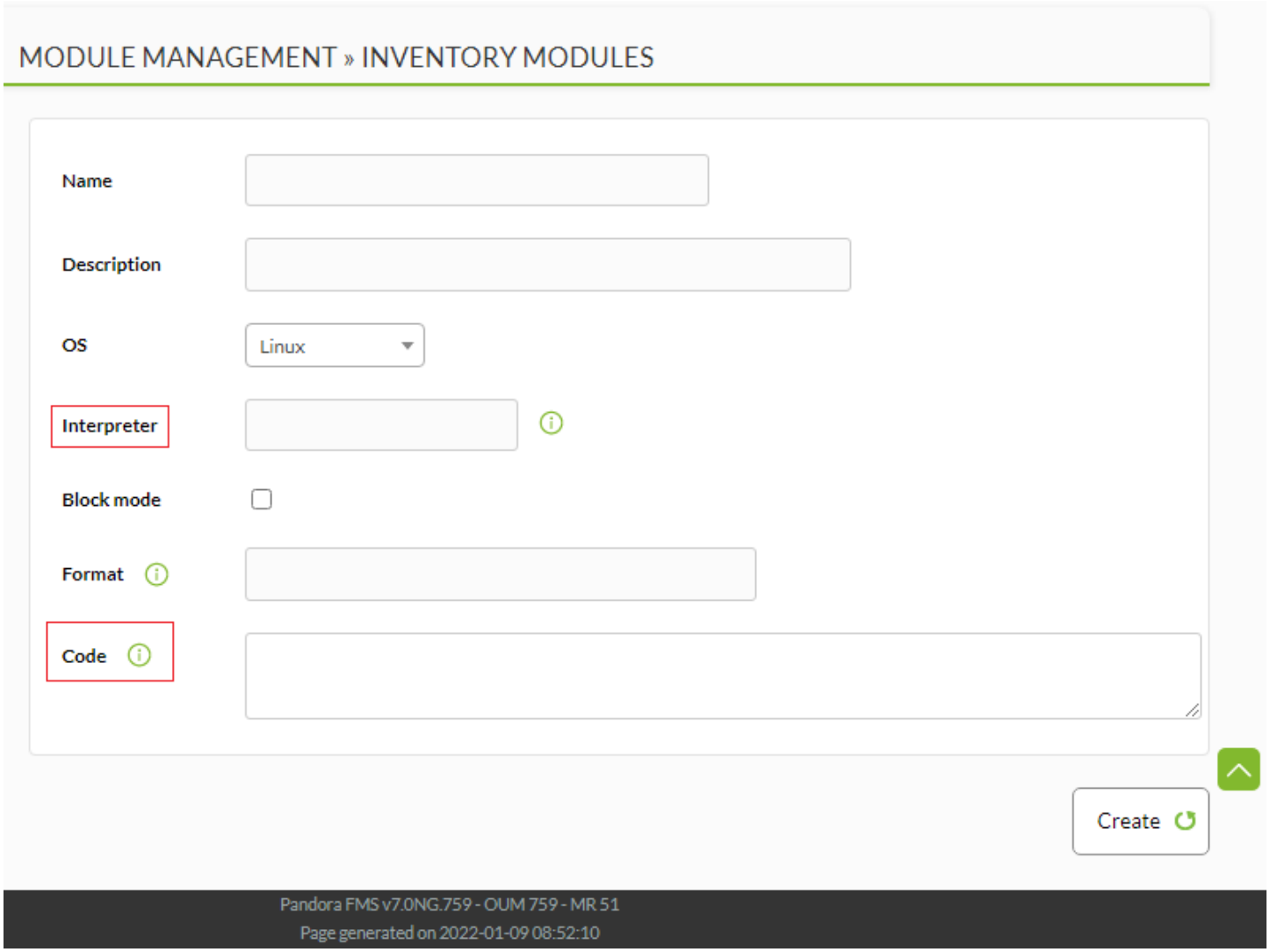
Как и в случае с удаленными модулями, эти модули также необходимо добавить в качестве инвентарных модулей в Configuration → Inventory modules.

Создание локальных модулей

Чтобы создать локальный модуль, перейдите в раздел Configuration → Inventory modules, где перечислены все созданные модули инвентаризации. Здесь должны быть созданы все модули, определенные в конфигурации агента; операционная система, назначенная агенту в консоли, также должна совпадать с операционной системой созданного модуля.

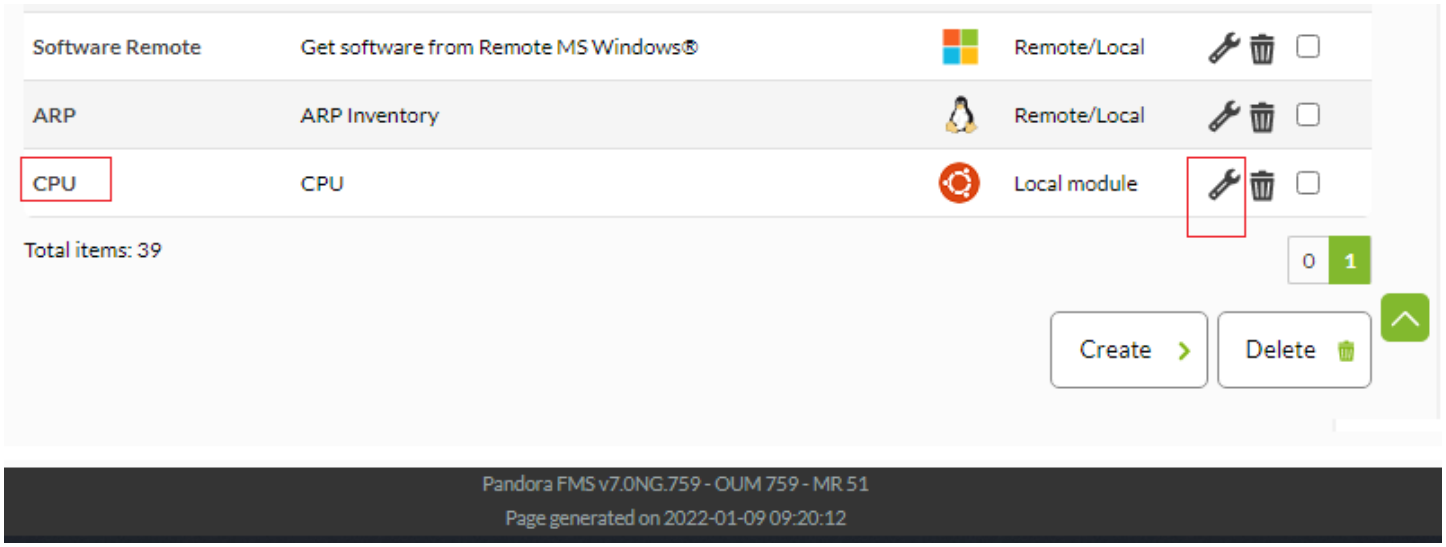


Чтобы создать новый модуль, нажмите на Create.

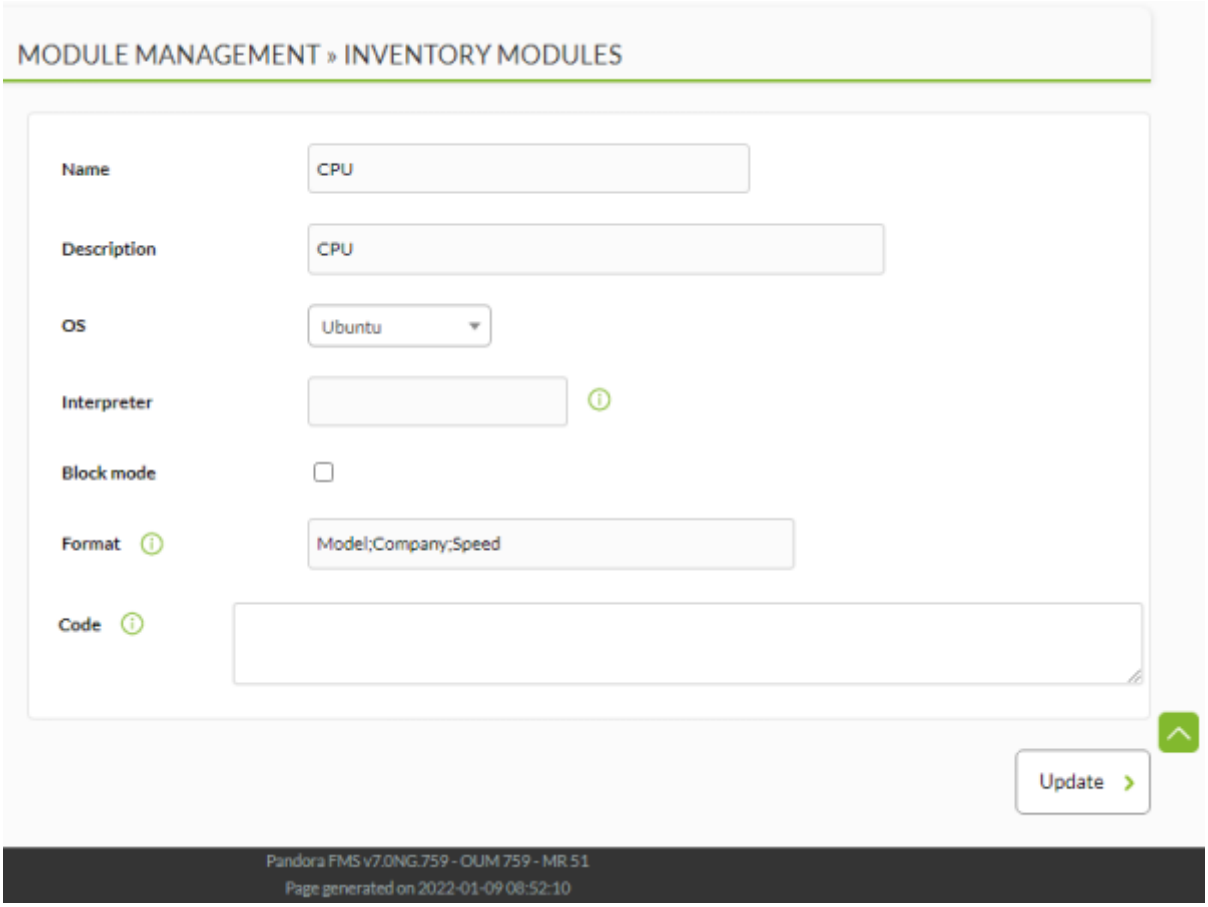


Процедура такая же, как и для случая с удаленным модулем, за исключением заполнения полей Interpreter и Code. В данном примере для поля OS можно задать собственные операционные системы.

После заполнения полей нажмите кнопку Создать, чтобы сохранить. В списке модулей инвентаризации вы увидите что-то вроде этого изображения:



Pour modifier le module d'inventaire nouvellement créé (ainsi que tous les autres), cliquez soit sur son nom, soit sur l'icône de la clé à molette.



Измените необходимые значения и нажмите кнопку Обновить, чтобы сохранить изменения.

Конфигурация локальной инвентаризации для программных агентов

Чтобы адаптировать конфигурацию программного агента к новой версии, необходимо:

1. Разверните коллекцию *скриптов* (загрузите из библиотеки Pandora FMS).

Начиная с версии 7, эти плагины по умолчанию поставляются вместе с установкой агента, хотя они закомментированы в конфигурационном файле.

2. Настройте запланированное выполнение *скриптов* локальной инвентаризации в файле `pandora_agent.conf`, добавив в конце следующую информацию:

Начиная с версии 7 и далее, нет необходимости в добавлении; просто откомментируйте существующие

плагины в конфигурационном файле Агента. Более подробную информацию можно найти в видеоуроке «Inventory modules in Windows» (повествование ведется на английском языке).

Пример для MS Windows®:

```
#module_begin
#module_plugin cscript.exe //B //t:20
"%PROGRAMFILES%\Pandora_Agent\util\cpuinfo.vbs"
#module_crontab * 12-15 * * 1
#module_end

#module_begin
#module_plugin cscript.exe //B //t:20
"%PROGRAMFILES%\Pandora_Agent\util\moboinfo.vbs"
#module_crontab * 12-15 * * 1
#module_end

#module_begin
#module_plugin cscript.exe //B //t:20
"%PROGRAMFILES%\Pandora_Agent\util\diskdrives.vbs"
#module_crontab * 12-15 * * 1
#module_end

#module_begin
#module_plugin cscript.exe //B //t:20
"%PROGRAMFILES%\Pandora_Agent\util\cdromdrives.vbs"
#module_crontab * 12-15 * * 1
#module_end

#module_begin
#module_plugin cscript.exe //B //t:20
"%PROGRAMFILES%\Pandora_Agent\util\videocardinfo.vbs"
#module_crontab * 12-15 * * 1
#module_end

#module_begin
#module_plugin cscript.exe //B //t:20
"%PROGRAMFILES%\Pandora_Agent\util\ifaces.vbs"
#module_crontab * 12-15 * * 1
#module_end

#module_begin
#module_plugin cscript.exe //B //t:20
"%PROGRAMFILES%\Pandora_Agent\util\monitors.vbs"
#module_crontab * 12-15 * * 1
#module_end
```

```
#module_begin
#module_plugin cscript.exe //B //t:20
"%PROGRAMFILES%\Pandora_Agent\util\printers.vbs"
#module_crontab * 12-15 * * 1
#module_end

#module_begin
#module_plugin cscript.exe //B //t:20
"%PROGRAMFILES%\Pandora_Agent\util\raminfo.vbs"
#module_crontab * 12-15 * * 1
#module_end

#module_begin
#module_plugin cscript.exe //B //t:20
"%PROGRAMFILES%\Pandora_Agent\util\software_installed.vbs"
#module_crontab * 12-15 * * 1
#module_end

#module_begin
#module_plugin cscript.exe //B //t:20
"%PROGRAMFILES%\Pandora_Agent\util\userslogged.vbs"
#module_crontab * 12-15 * * 1
#module_end

#module_begin
#module_plugin cscript.exe //B //t:20
"%PROGRAMFILES%\Pandora_Agent\util\productkey.vbs"
#module_crontab * 12-15 * * 1
#module_end

#module_begin
#module_plugin cscript.exe //B //t:20
"%PROGRAMFILES%\Pandora_Agent\util\productID.vbs"
#module_crontab * 12-15 * * 1
#module_end
```

Модуль инвентаризации в системах Unix с помощью программного агента

Модуль программного агента Unix локально использует *плагин* для сбора информации о различных аспектах машины, как программных, так и аппаратных.

Синтаксис модуля следующий:

```
module_plugin inventory 1 cpu ram video nic hd cdrom software init_services
filesystem users route
```

Модуль состоит из строки со следующими параметрами:

- Активация модуля:

```
"module_plugin inventory" 1 cpu ram video nic hd cdrom software init_services
filesystem users route
```

- Поле, в котором устанавливается, с какой периодичностью (в днях) будет выполняться модуль. Если ноль (0), то инвентарь возвращается при каждом выполнении Агента.

```
module_plugin inventory "1" cpu ram video nic hd cdrom software init_services
filesystem users route
```

- Поле, в котором задаются объекты инвентаризации, подлежащие сбору.

```
module_plugin inventory 1 "cpu ram video nic hd cdrom software init_services
filesystem users route"
```

Как и в агенте для MS Windows®, можно собирать следующие объекты:

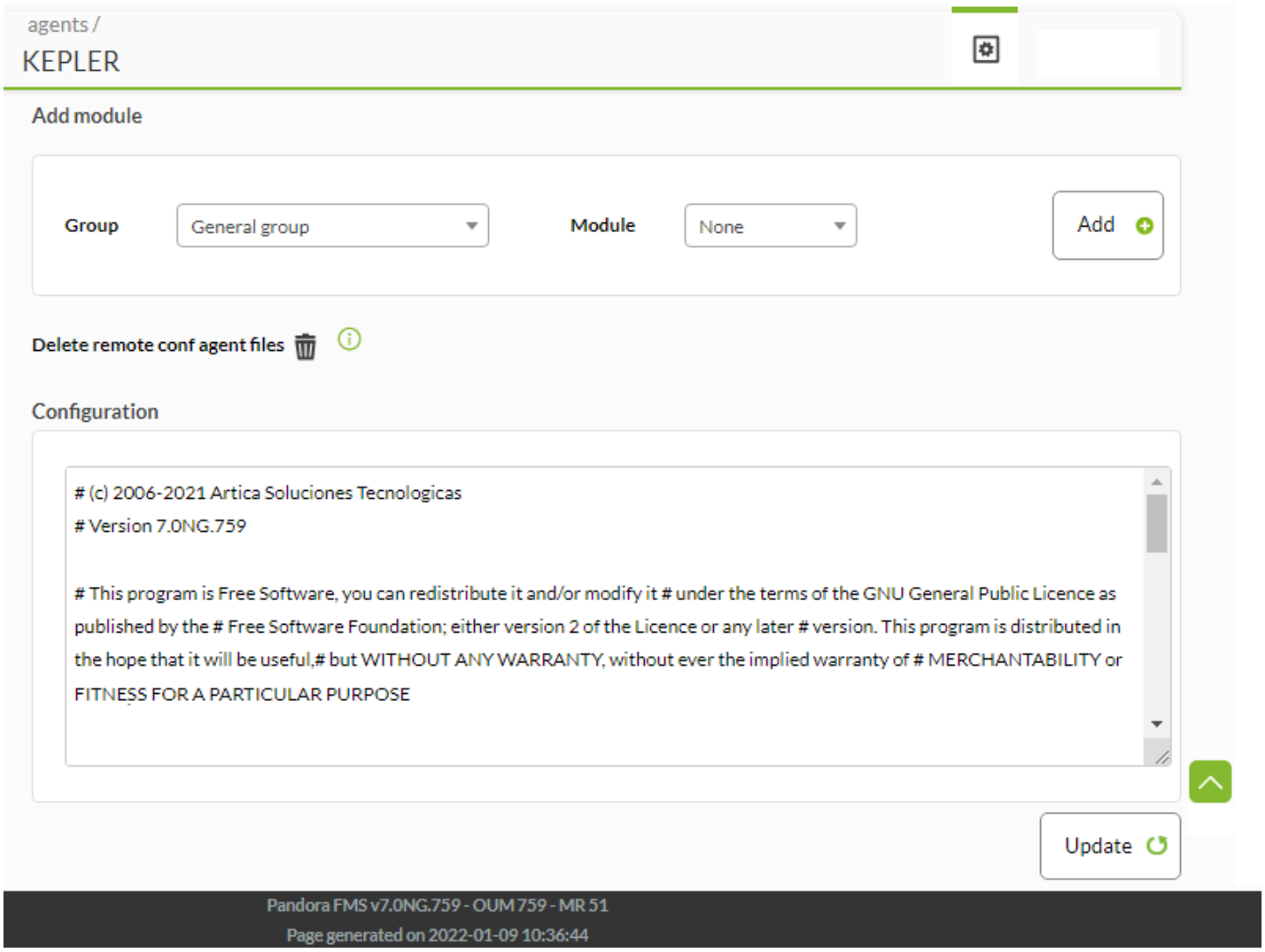
- CPU: Собирает информацию о центральных процессорах.
- ram: Собирает информацию о модулях оперативной памяти.
- video: Собирает информацию о видеокартах.
- nic: Собирает информацию о сетевых картах, Network Interface Controlers.
- hd: Собирает информацию о жестких дисках.
- cdrom: Собирает информацию об устройствах чтения оптических дисков.
- patches: Собирает информацию об установленных программных *патчах*.
- software: Собирает информацию об установленном программном обеспечении.
- init_services: Собирает информацию о процессах авто инициирования.
- filesystem: Собирает информацию о сегментации системы.
- users: Собирает информацию о пользователях.
- Route: Собирает информацию о таблице путей системы.

Плагин, который собирает инвентарь, находится в каталоге `/etc/pandora/plugins`.

Он также может быть задан просто для сбора всей доступной информации. В данном примере он ежедневно собирает всю информацию об инвентаризации:

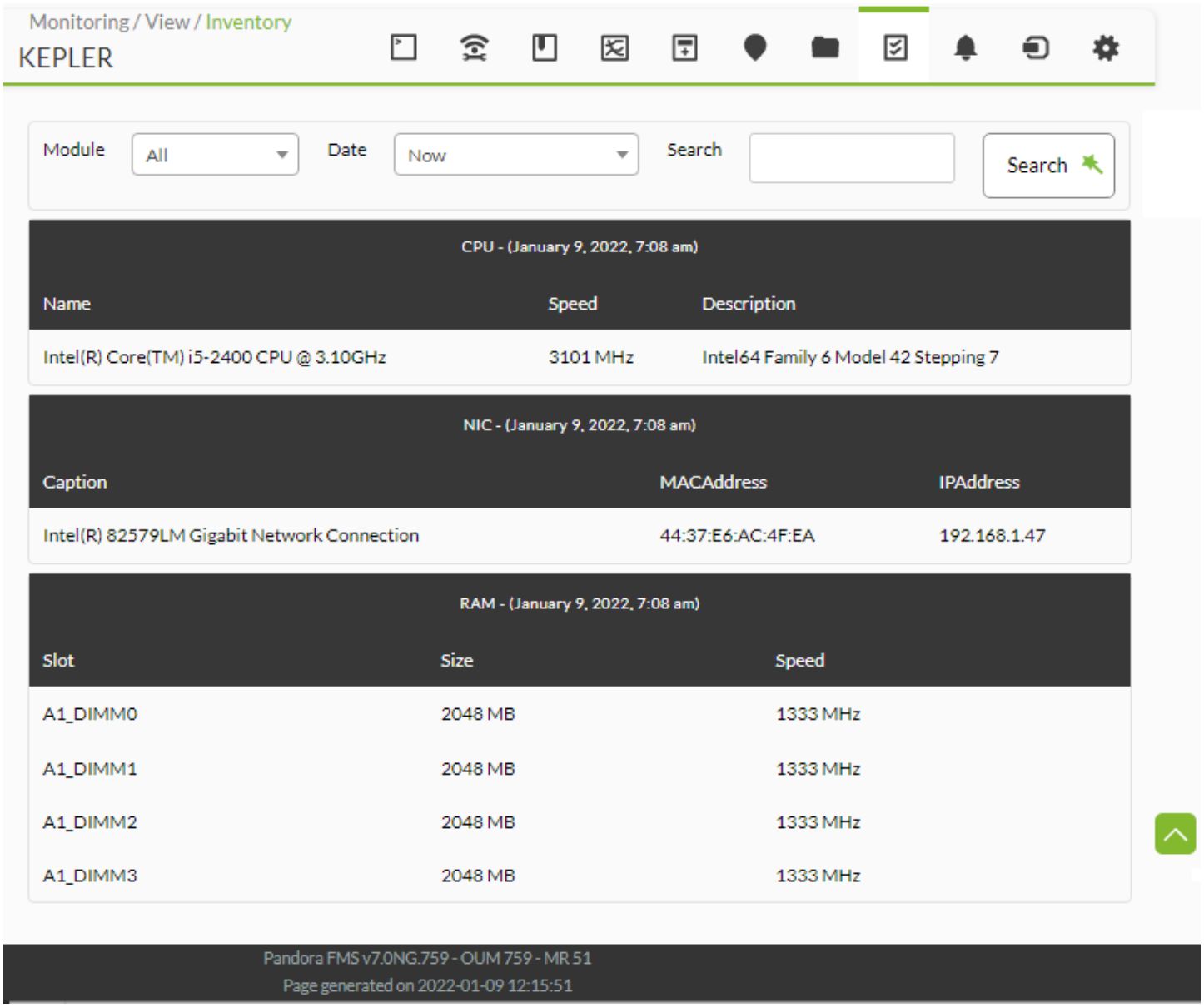
```
# Plugin for inventory on the agent (Only Enterprise)
module_plugin inventory 1
```

Чтобы активировать модуль инвентаризации, просто скопируйте описанный выше код в файл `pandora_agent.conf` программного агента, а затем перезапустите службу. Эта активация может быть из удаленной конфигурации агента (ьолее подробную информацию можно найти в видеоуроке «Inventory modules in Windows» (повествование ведется на английском языке) или выполнена локально:



Назначение локальных модулей

Нет необходимости активировать модули в агентах, определенных в консоли. Если модули были созданы в Configuration → Inventory modules, операционная система соответствует, а выполнение определено в конфигурационном файле программного агента *собранные данные появятся напрямую* в разделе View → Inventory агента в консоли.



Создание локальных модулей инвентаризации с помощью Software Agent

В дополнение к системам инвентаризации, предварительно настроенным в Агенте, вы можете легко создавать модули инвентаризации для систем Unix® и Windows®.

В основном вам нужно создать *скрипт*, который генерирует XML со следующей структурой:

```
<inventory>
<inventory_module>
<name>INVENTORY_MODULE_NAME</name>
<type>generic_data_string</type>
<datalist>
    <data>DATA1;DATA2;DATA3....</data>
</datalist>
</inventory_module>
</inventory>
```

INVENTORY_MODULE_NAME: Вы должны поместить то же имя модуля, которое вы

зарегистрировали в модулях инвентаризации в консоли Pandora FMS.

DATA1;DATA2... : Это данные, которые необходимо извлечь и которые были определены в модуле инвентаризации.

Предположим, вы хотите получить ARP-таблицу, IP-адрес с его интерфейсами (см. предыдущий пример с удаленными модулями инвентаризации). Используйте команду `arp -a` и очистите запись, чтобы получить нужные данные.

Теперь для разработки в MS Windows® сделайте небольшой *скрипт* `C:\tmpwindows_arp_inventory.bat` со следующим определением:

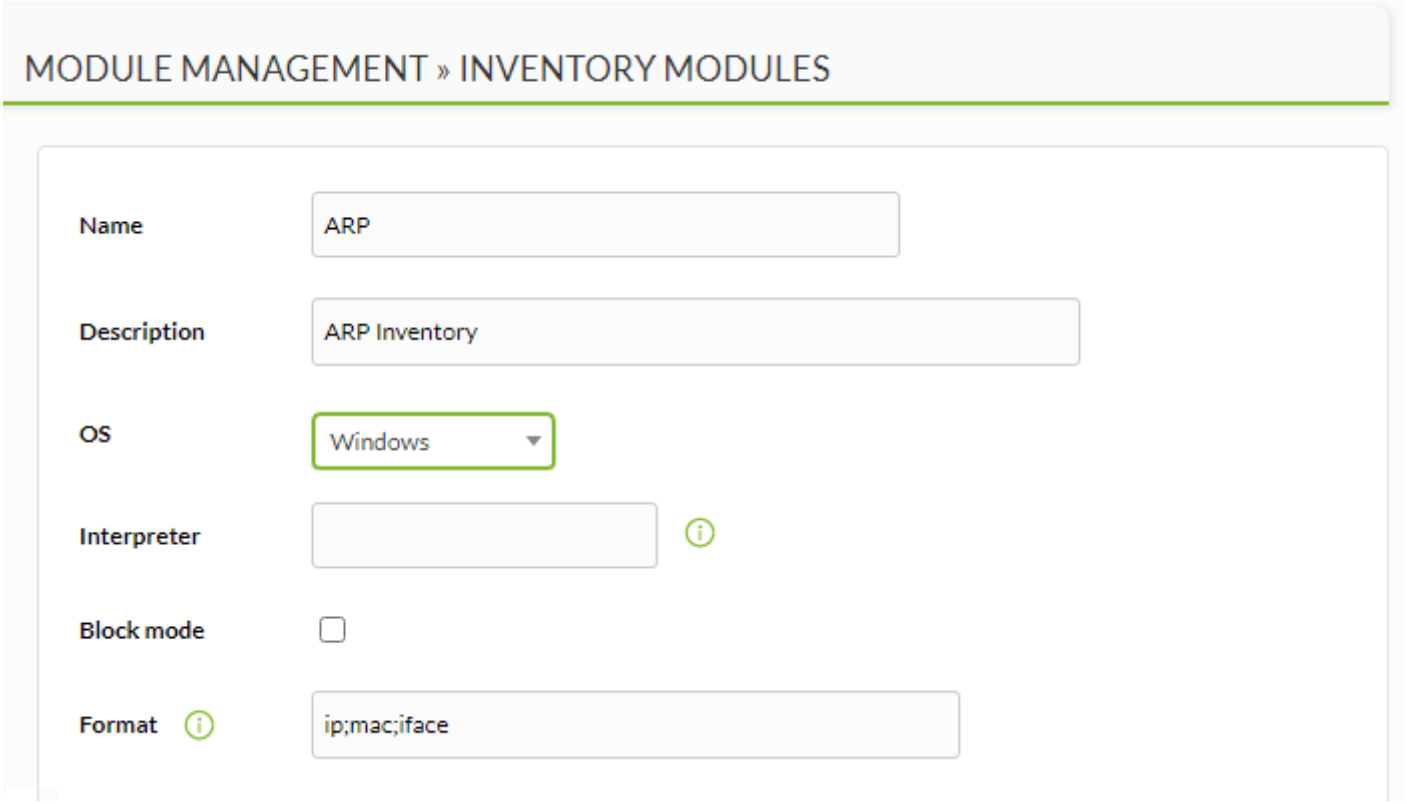
```
@echo off

echo ^<inventory^>
echo ^<inventory_module^>
echo ^<name^>ARP^</name^>
echo ^<type^>generic_data_string^</type^>
echo ^<datalist^>
arp -a | sort | grep "[0-9]"  | grep -v ":" | gawk "{ print \"^<data^>\"
$1\";\"$2\";\"$3 \"^</data^>\" }"
echo ^</datalist^>
echo ^</inventory_module^>
echo ^</inventory^>
```

Теперь вам нужно изменить `pandora_agent.conf`, и добавить следующую строку:

```
module_plugin cmd.exe /C C:\tmp\windows_arp_inventory.bat
```

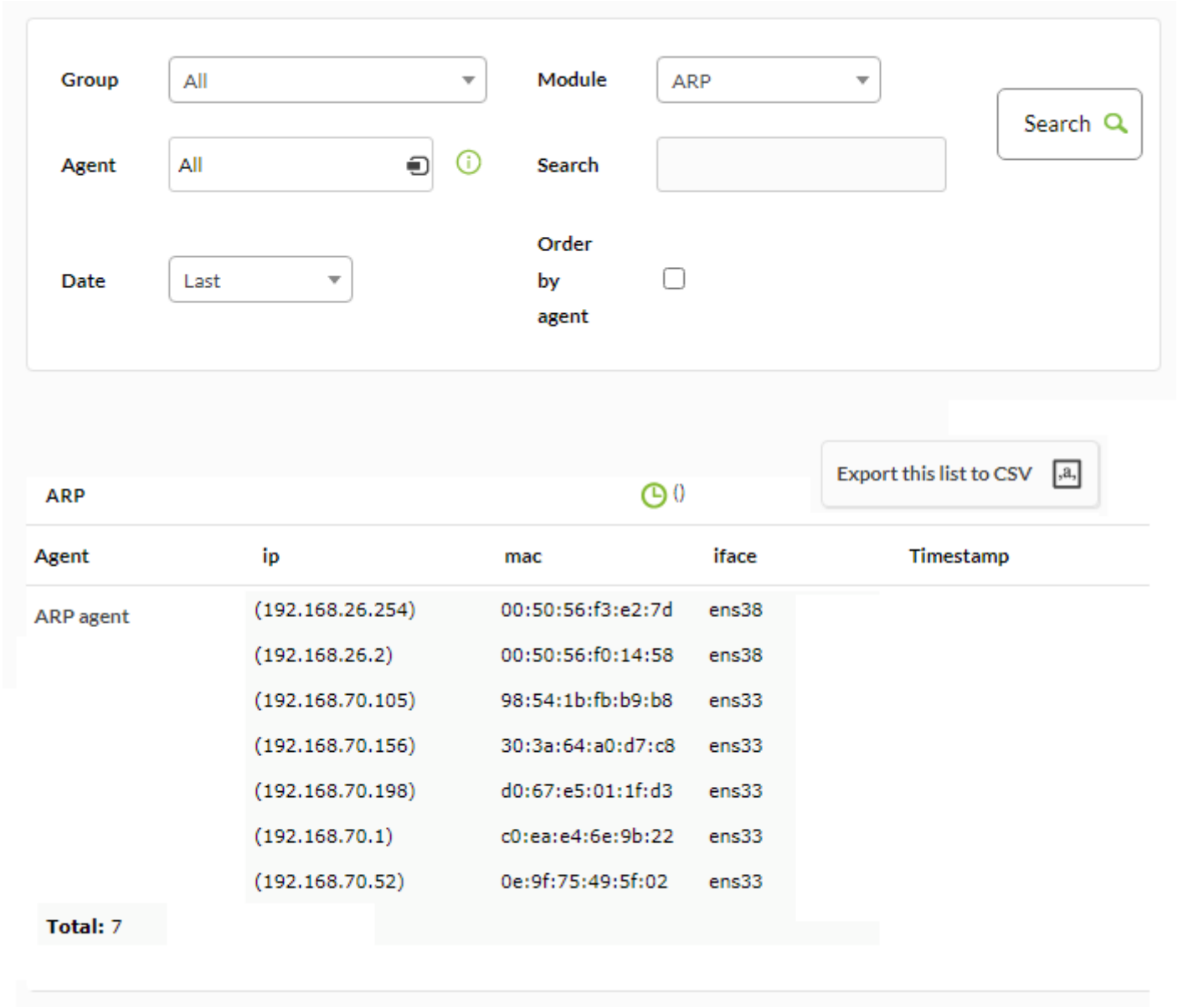
Этот скрипт будет запускаться каждые 5 минут (по умолчанию - это интервал Агента). Если вы хотите, чтобы он запускался каждые X времени, вам придется реализовать эту логику в самом *скрипте* или использовать запланированный мониторинг

Помните: чтобы локальный *script* мог хранить информацию об инвентаризации, в консоли должен быть определен модуль инвентаризации, в котором указывается операционная система, имя модуля и данные для хранения, разделенные `;` . Помните, что перед перезапуском агента Pandora FMS, чтобы загрузить внесенные изменения, создайте модуль инвентаризации в Pandora FMS:



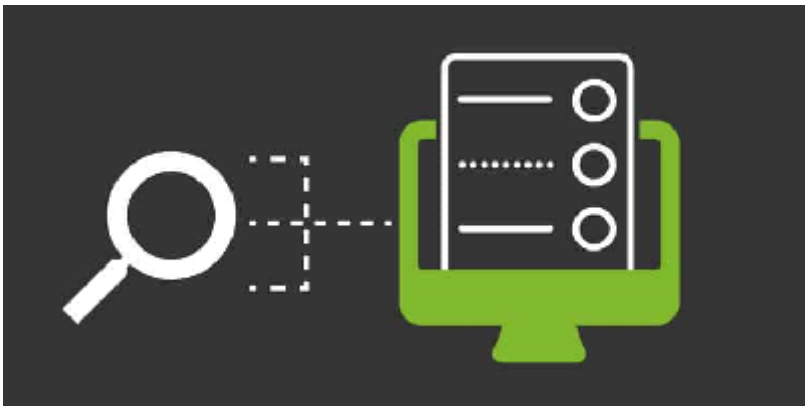
Обратите внимание, что, будучи локальным модулем, поля Interpreter и Code не нужны, хотя поле Operating System (OS) важно.

Полученные результаты совпадают с результатами, полученными для эквивалентного удаленного модуля в GNU Linux:



В онлайн-библиотеке модулей Pandora FMS имеется множество других модулей инвентаризации, как удаленных, так и локальных. Вы также можете легко разрабатывать свои собственные модули, как вы уже видели в этой главе.

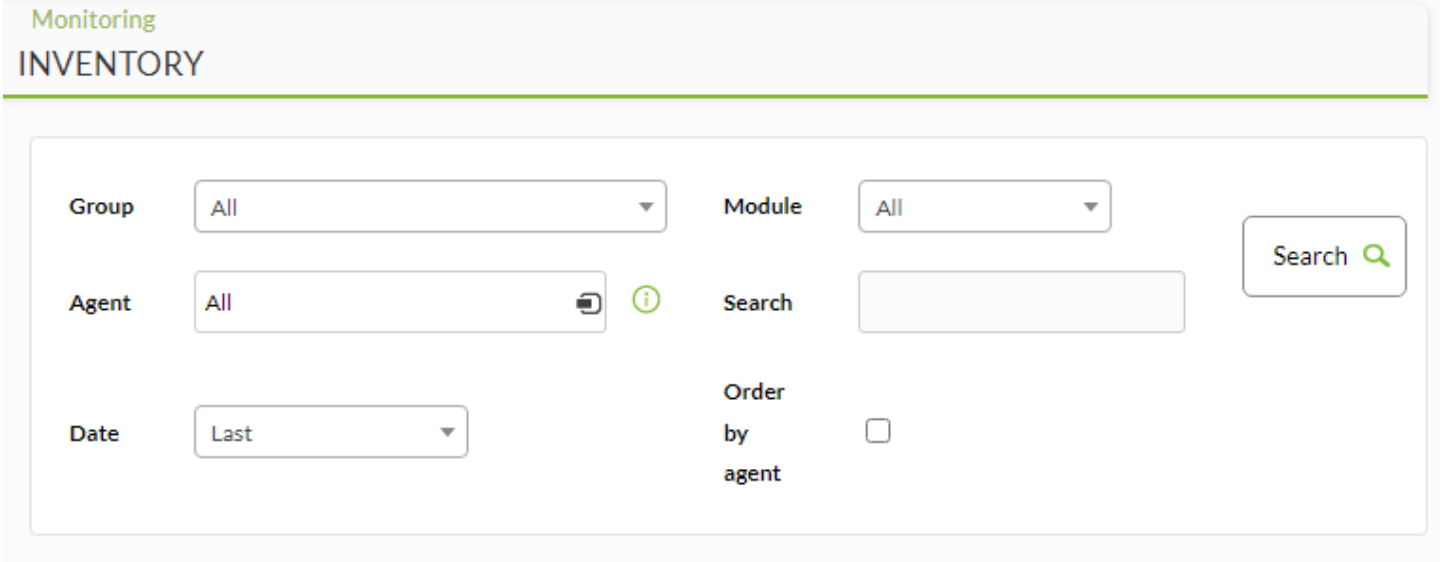
Визуализация данных инвентаризации



Данные инвентаризации, собранные из системы, локально или удаленно, можно просмотреть из самого агента или из меню Инвентаря консоли.

Просмотр данных инвентаризации в меню Инвентаря

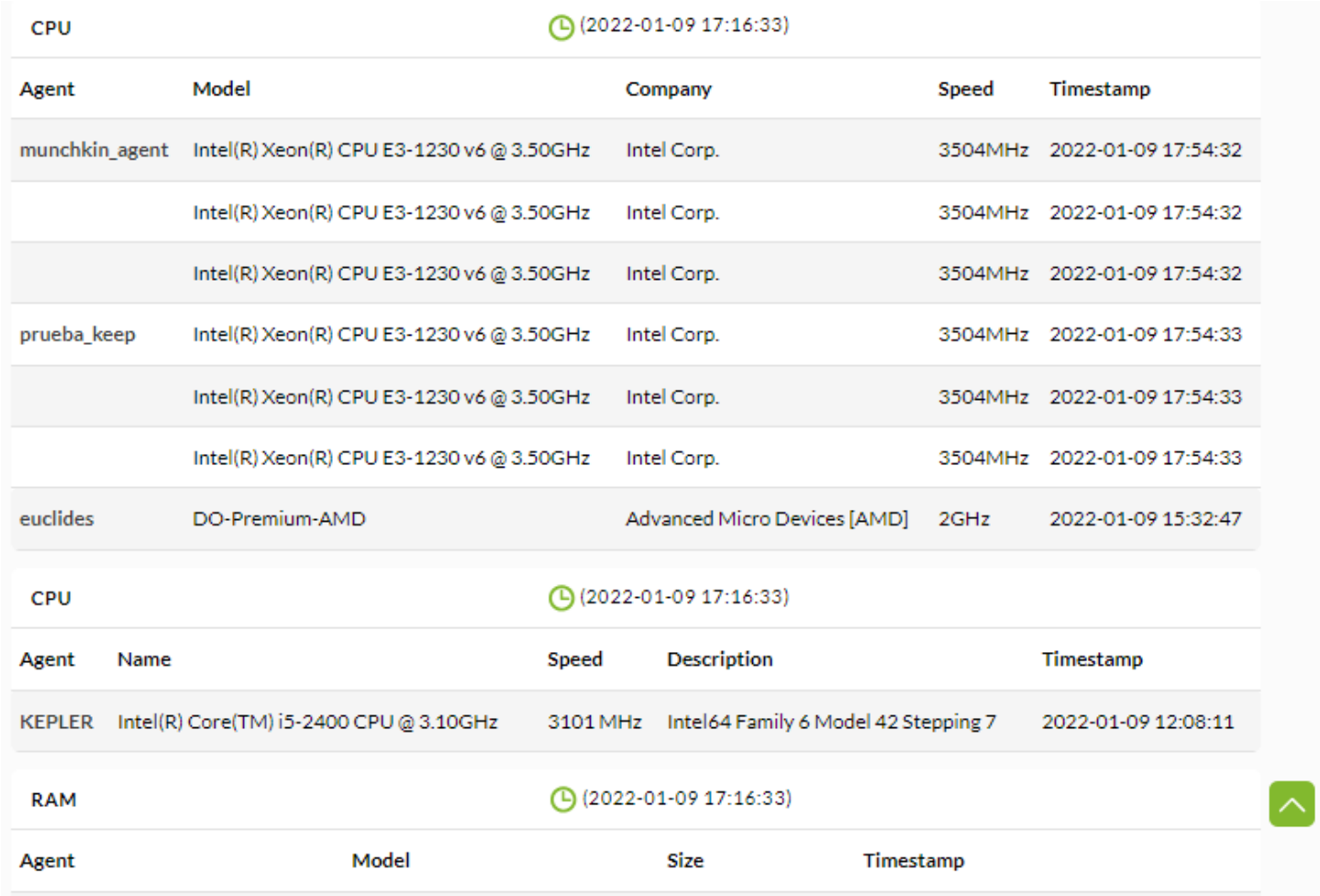
В разделе Monitoring → Inventory можно просмотреть данные инвентаризации всех агентов, выполнить поиск и экспортировать данные в CSV-файл.



Ниже перечислены поля, которые можно использовать для поиска.

- Group: Выберите группу агентов для фильтрации. Пользователь сможет увидеть группы, к которым он будет принадлежать, только если этот пользователь не принадлежит к группе ВСЕ (ALL).
- Module: Выберите модуль инвентаризации, по которому вы хотите отфильтровать данные.
- Agent: Введите имя агента, по которому вы хотите отфильтровать.
- Search: Напишите текст для поиска по всем полям инвентаря.

С помощью поиска можно просмотреть модули всех агентов, у которых есть инвентарь, выбрав в параметрах поиска все и нажав на Search.



CPU (2022-01-09 17:16:33)

Agent	Model	Company	Speed	Timestamp
munchkin_agent	Intel(R) Xeon(R) CPU E3-1230 v6 @ 3.50GHz	Intel Corp.	3504MHz	2022-01-09 17:54:32
	Intel(R) Xeon(R) CPU E3-1230 v6 @ 3.50GHz	Intel Corp.	3504MHz	2022-01-09 17:54:32
	Intel(R) Xeon(R) CPU E3-1230 v6 @ 3.50GHz	Intel Corp.	3504MHz	2022-01-09 17:54:32
prueba_keep	Intel(R) Xeon(R) CPU E3-1230 v6 @ 3.50GHz	Intel Corp.	3504MHz	2022-01-09 17:54:33
	Intel(R) Xeon(R) CPU E3-1230 v6 @ 3.50GHz	Intel Corp.	3504MHz	2022-01-09 17:54:33
	Intel(R) Xeon(R) CPU E3-1230 v6 @ 3.50GHz	Intel Corp.	3504MHz	2022-01-09 17:54:33
euclides	DO-Premium-AMD	Advanced Micro Devices [AMD]	2GHz	2022-01-09 15:32:47

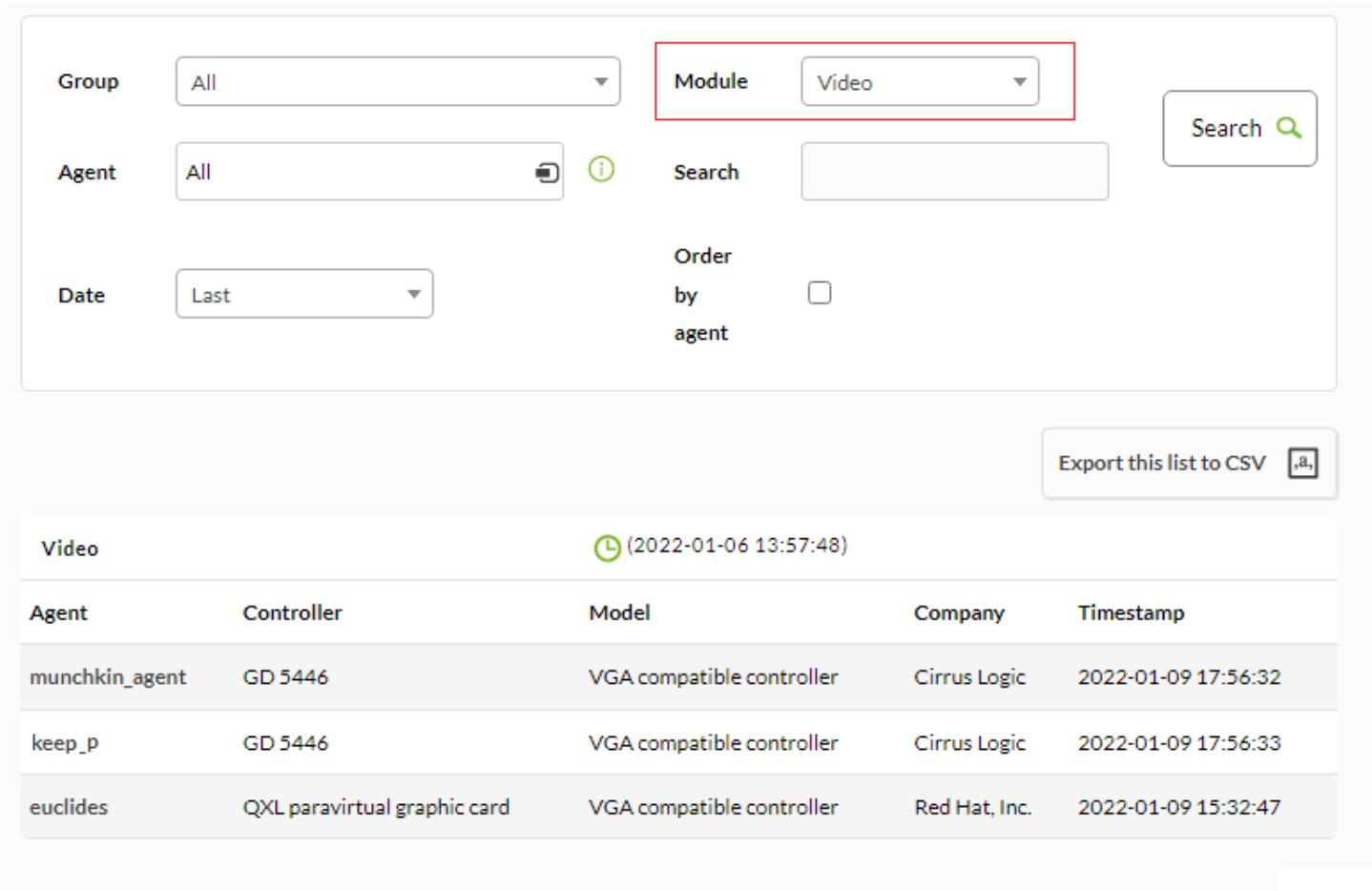
CPU (2022-01-09 17:16:33)

Agent	Name	Speed	Description	Timestamp
KEPLER	Intel(R) Core(TM) i5-2400 CPU @ 3.10GHz	3101 MHz	Intel64 Family 6 Model 42 Stepping 7	2022-01-09 12:08:11

RAM (2022-01-09 17:16:33)

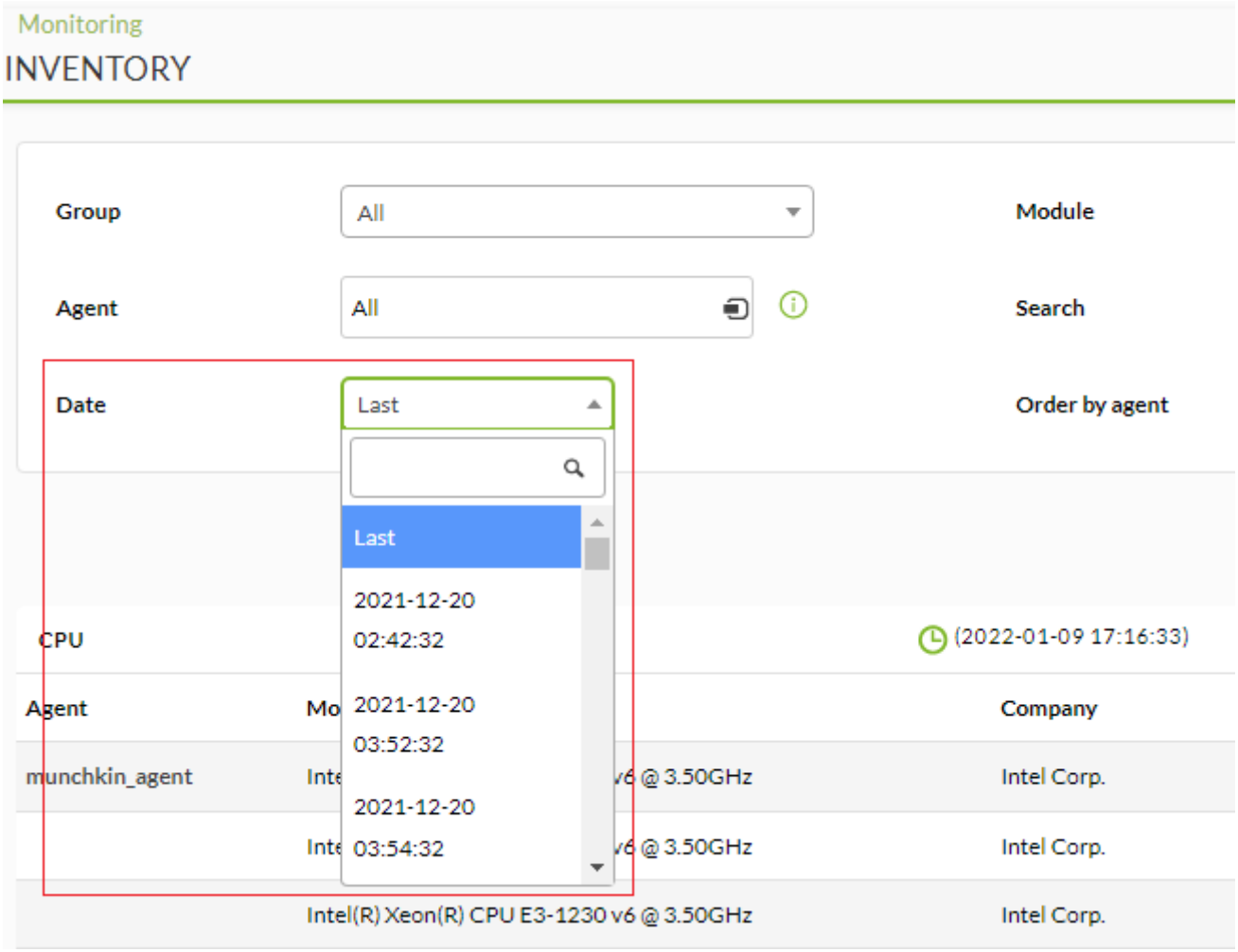
Agent	Model	Size	Timestamp

Или конкретный модуль всех агентов с инвентарем, выбрав модуль и нажав на Search.



Даты и изменения в инвентаризации

В подробном просмотре инвентаризации агента с помощью селектора можно выбрать дату отображения конкретного отчета об инвентаризации:

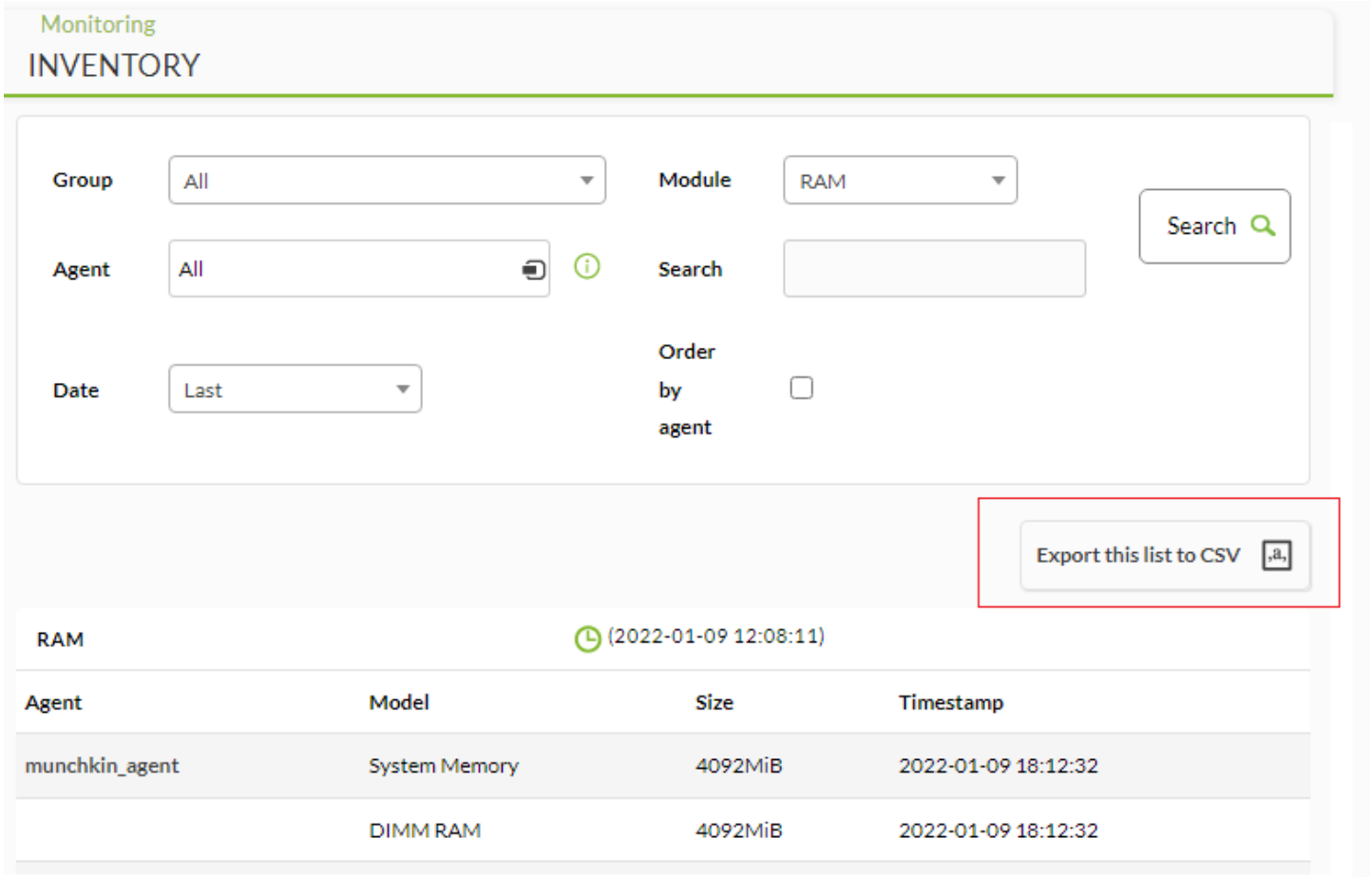


Если вы заметили, что даты отсутствуют, это, вероятно, потому, что в данные не изменились после последнего выполнения инвентаризации. *То есть, Pandora FMS сохраняет данные инвентаризации только тогда, когда они изменяются после последнего выполнения*

Экспорт данных инвентаризации в CSV

Через Monitoring → Inventory можно экспортировать данные инвентаризации, полученные в результате фильтрации, в CSV-файл.

Выберите фильтр и, когда данные будут доступны, выберите Export this list to CSV.



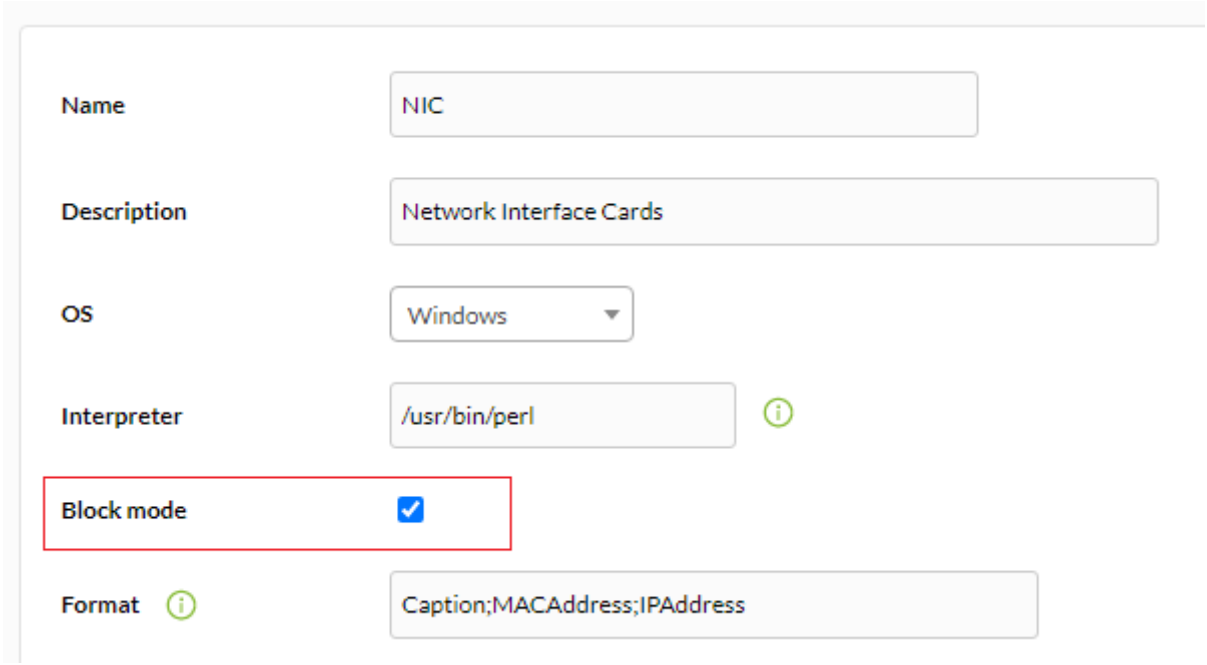
Создается файл с данными инвентаризации, разделенные точкой с запятой.

Различия между версиями инвентаризации

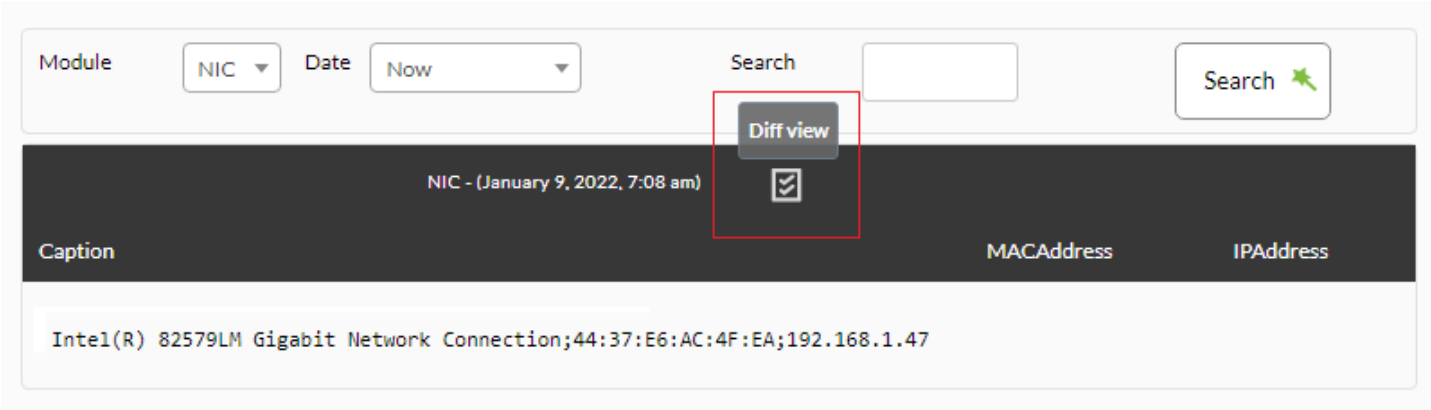
Режим блоков

В версии Pandora 5.1 можно наглядно показать различия между двумя конфигурациями, отображая их в двух колонках, чтобы увидеть разницу. Режим блоков указывает, что результатом модуля инвентаризации является один элемент, а не интерпретирует каждую строку как различные элементы одного типа, как это было сделано в модулях инвентаризации, рассмотренных выше.

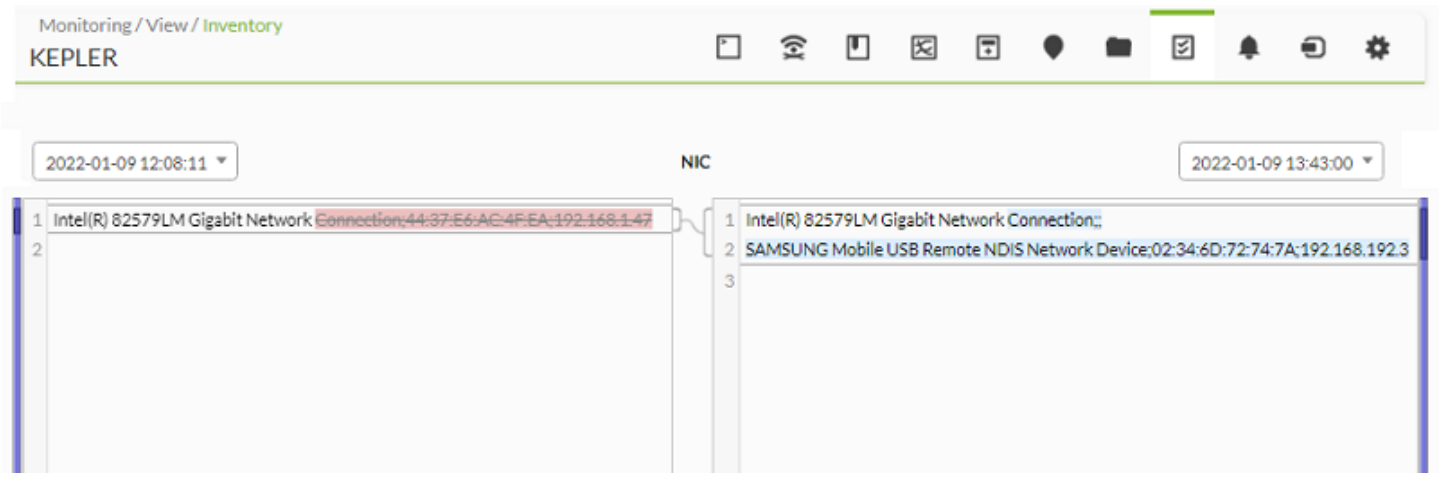
Блочный режим настраивается (Block mode) при определении локального или удаленного модуля инвентаризации:



Когда модуль настроен в блочном режиме, он позволяет просматривать его по секциям(для визуального наблюдения за изменениями).

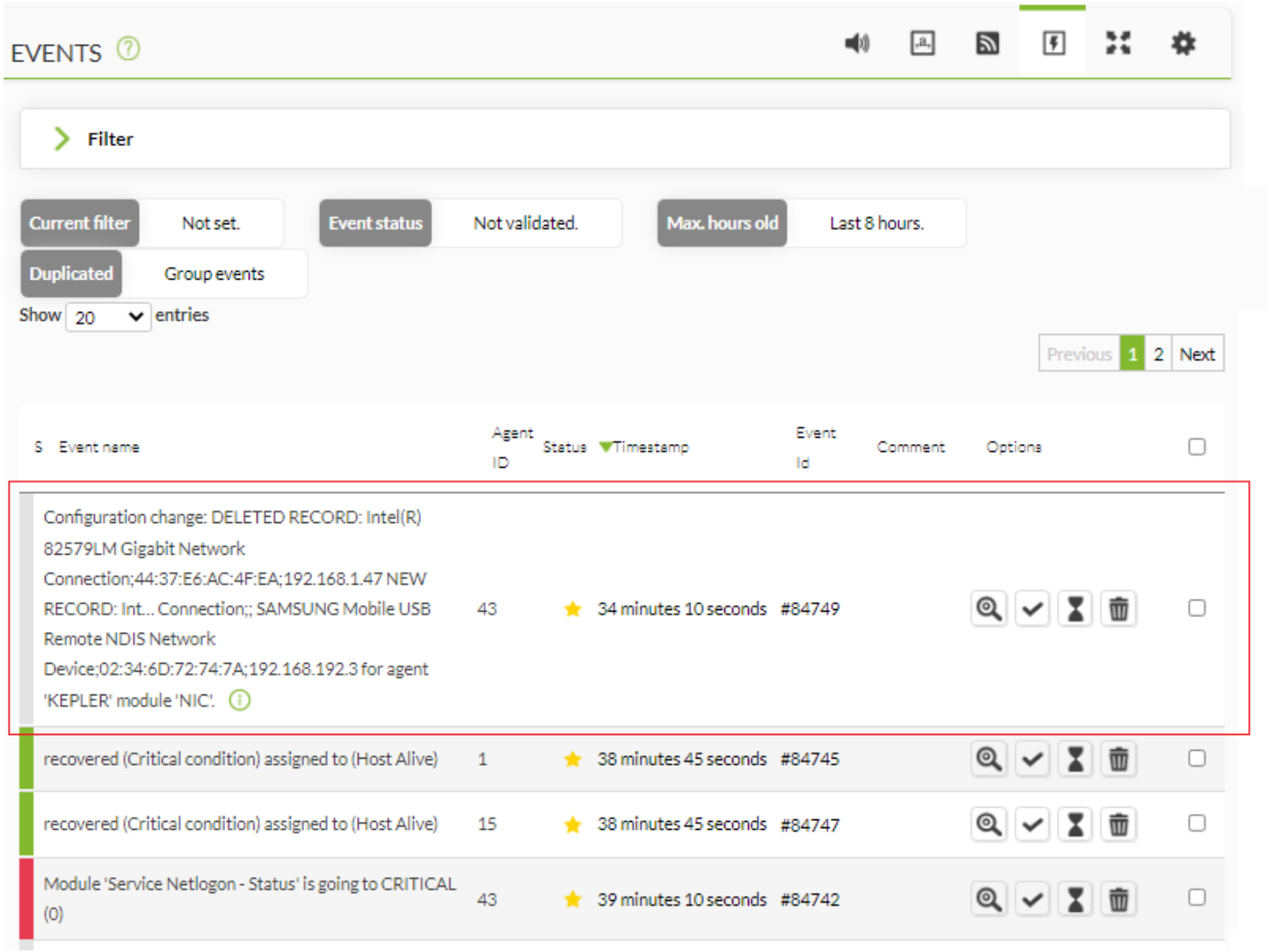


Представление в виде двух колонок показывает различия между одной версией инвентаризации и другой, и вы даже можете выбрать версию по дате.



Помните, что каждый раз, когда обнаруживается изменение в модуле инвентаризации,

генерируется событие.

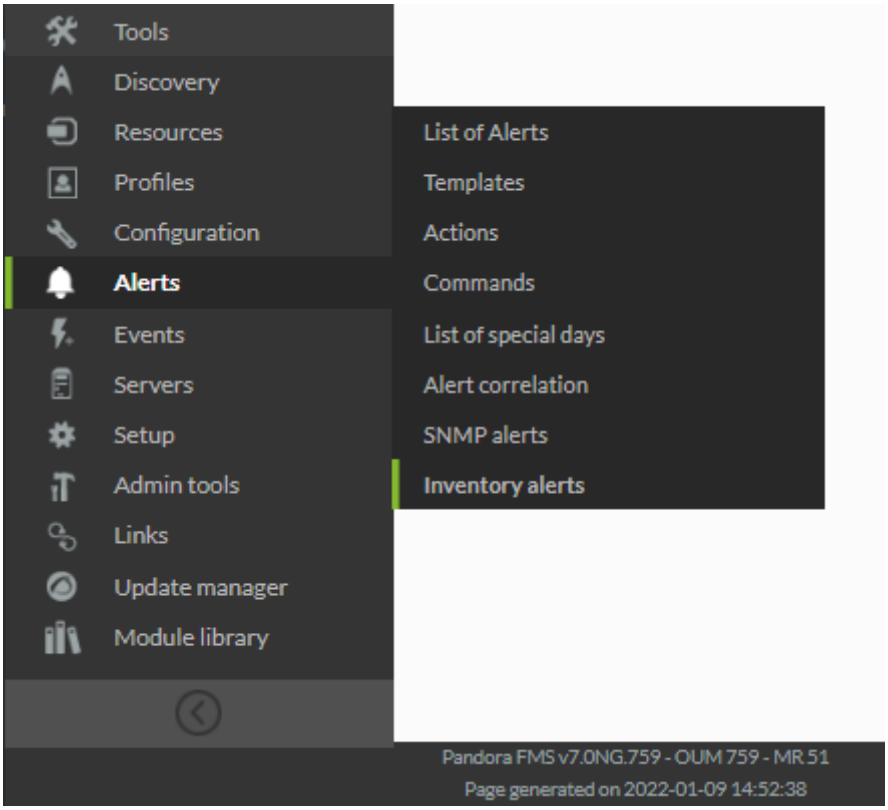


Предупреждения инвентаризации

Версия 751 NG или позже.

Предупреждения инвентаризации используются для запуска конкретных предупреждений о содержимом инвентаря группы агентов. Как и предупреждения SNMP или предупреждения о событиях, они не применяются агентом к агенту, а являются глобальными, в данном случае они применяются группами.

Чтобы установить их, необходимо перейти в раздел Alerts → Inventory alerts.



Предупреждения инвентаризации имеют поля, аналогичные другим предупреждениям, такие как имя, описание, *временной порог* и действие, как указано в главе о предупреждениях Pandora FMS. Здесь объяснены их различия./p>

- Группа в данном случае действует как условие предупреждения, так что предупреждения будут оцениваться для любых данных, поступающих от агента этой группы.
- Эти предупреждения также имеют опцию деактивировать событие, чтобы при срабатывании предупреждения не генерировалось событие предупреждения. Это полезно, так как возможно, что при применении инвентаризационных оповещений многие предупреждения могут срабатывать или включаться за одно выполнение.

Условие срабатывания предупреждения

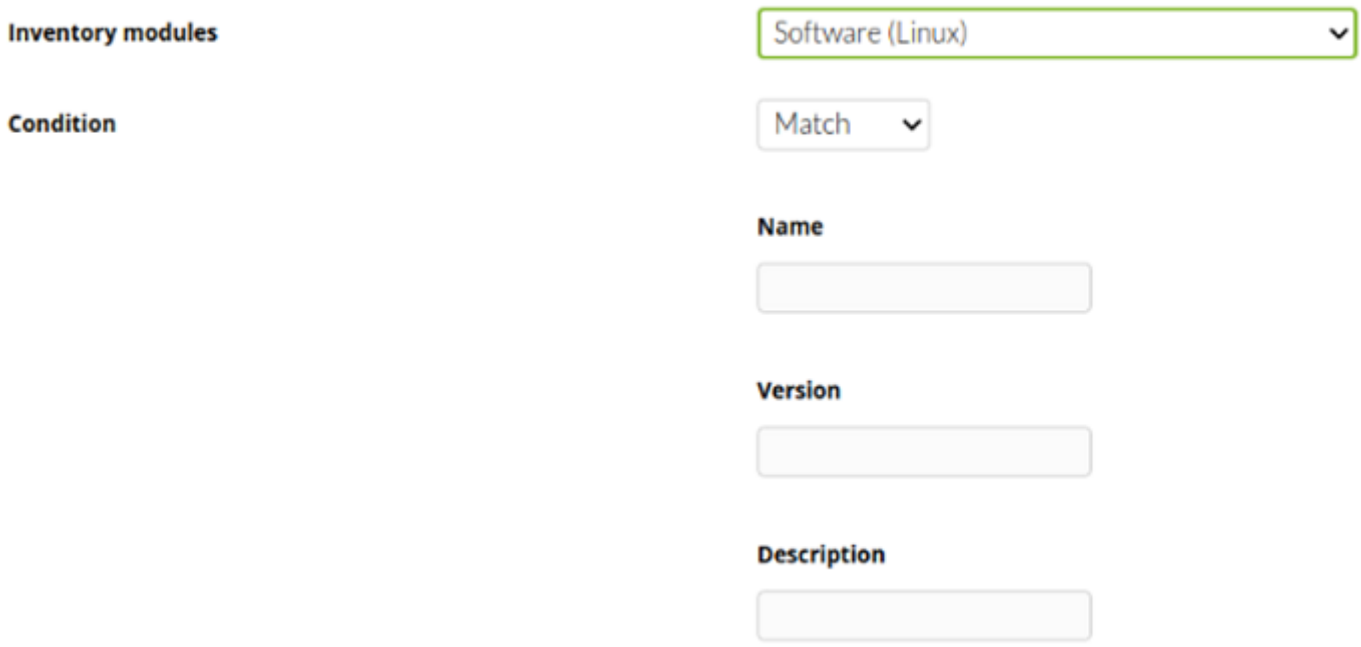
Предупреждения об инвентаризации оцениваются в трех различных режимах: сопоставление строк, разрешенный список и ограниченный список.

Сопоставление текстовых строк

В этом режиме, если определенная строка поступает в определенный модуль инвентаризации, например, “software”, срабатывает установленное действие. Следует отметить, что модули инвентаризации имеют динамические поля; т.е. в модуле инвентаризации программного обеспечения есть поле имени, версия и описание:

serpentis	acl	2.2.51	Access control list utilities
	aic94xx-firmware	30	Adaptec SAS 44300, 48300, 58300 Sequencer Firmware for AIC94xx driver
	alsa-firmware	1.0.28	Firmware for several ALSA-supported sound cards
	alsa-lib	1.1.6	The Advanced Linux Sound Architecture (ALSA) library
	alsa-tools-firmware	1.1.0	ALSA tools for uploading firmware to some soundcards
	apr	1.4.8	Apache Portable Runtime library
	apr-util	1.5.2	Apache Portable Runtime Utility library
	atk	2.28.1	Interfaces for accessibility support

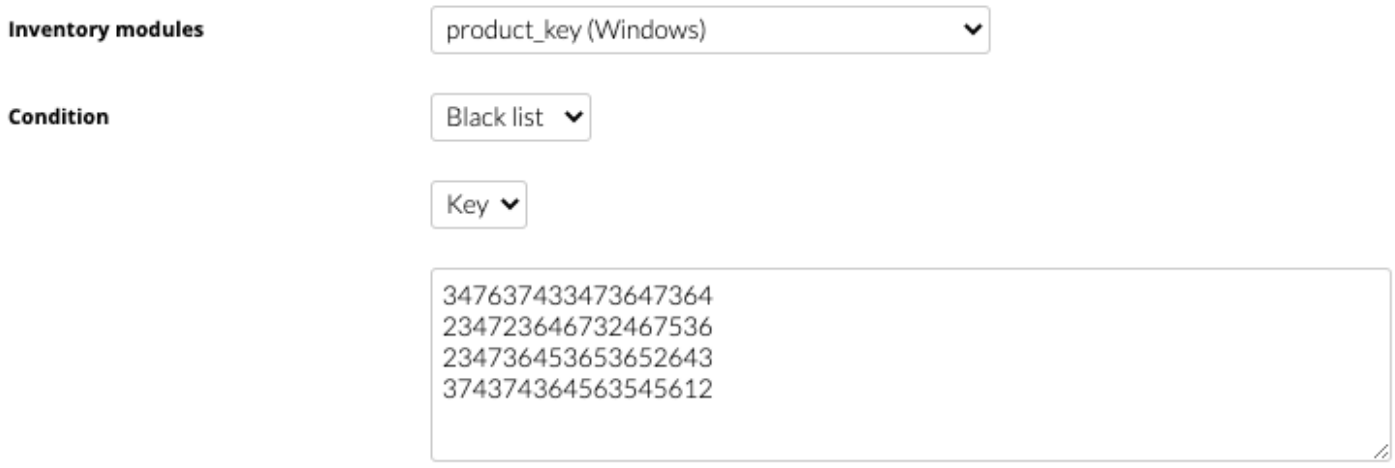
Таким образом, вы можете установить предупреждение для любого из трех динамических полей. Это идеальный вариант, если вы ищете конкретный пакет или пакет определенной версии:



Будут отображены все поля модуля инвентаризации. В этих полях вы можете использовать регулярные выражения для более сложного поиска. Если поле оставлено пустым, оно считается .* (оно покажет *match* или будет совпадать с любым значением).

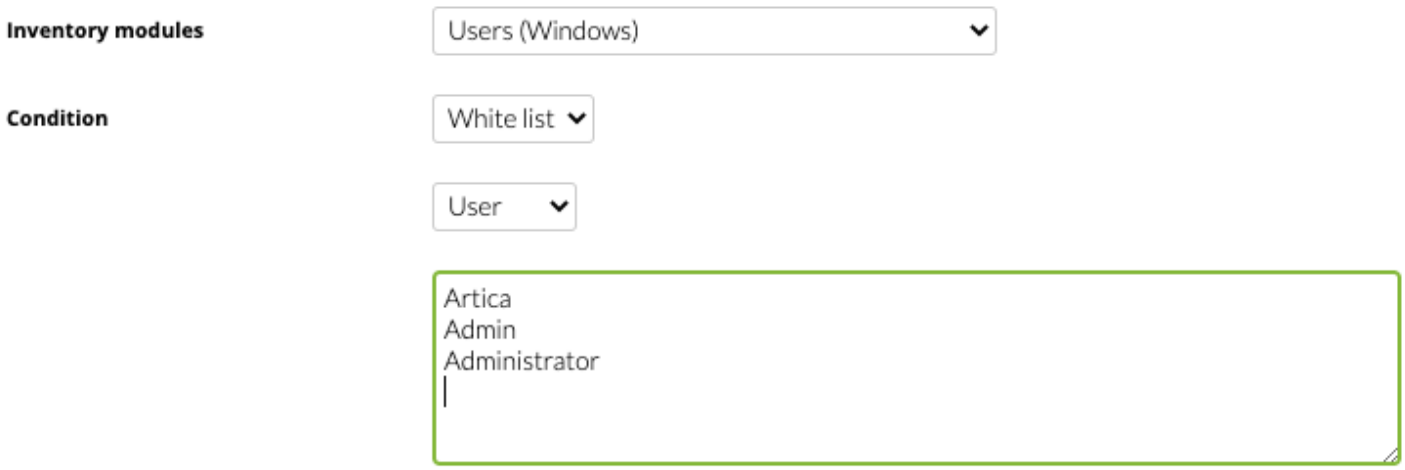
Ограниченный список

В этом случае вы должны указать только одно поле типа модуль инвентаризации и задать список строк (по одной на строку), чтобы, если агент содержит элемент из этого списка, сработало оповещение. Например, в случае программного обеспечения, этот ограниченный список (Black list) - это список пакетов программ, которые не должны быть установлены на машине. Если на машине установлен один из этих пакетов, сработает предупреждение.



Разрешенный список

Действует так же, как и в предыдущем случае. Укажите список элементов для одного из полей инвентаризации; однако, этом случае значение модуля инвентаризации должно всегда находиться в одном из элементов списка, *иначе сработает предупреждение.*



Использование предупреждений инвентаризации

Эта функция действительно полезна для обнаружения уязвимых версий устройств, неавторизованных пользователей на машинах или неавторизованного программного обеспечения на компьютерах.

Вернуться в оглавление Документации Pandora FMS