

Table of Contents

Table of Contents	1
Настройка библиотек	2
Настройка библиотек (Описание)	3

Documentation: ☒
Product: SIEM
Version: 7.1.x, 7.2.x

Настройка IP-адресов

Данный раздел находится на уровне **libraries ip-list**.
Для создания группы IP-адресов используется следующая команда:
Admin@nodename# create libraries ip-list <parameters>
Далее необходимо задать следующие параметры:

Параметр	Описание
name	Название списка адресов.
description	Описание списка.
threat-lvl	Уровень угрозы: • very-low — очень низкий уровень угрозы. • low — низкий уровень угрозы. • medium — средний уровень угрозы. • high — высокий уровень угрозы. • very-high — высокий уровень угрозы.
type	Тип списка: • local — локальный. • updatable — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (url). Периодичность обновления списка указывается параметром shedule в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".
lists	Выбор существующих IP-листов для добавления в создаваемый лист.
ips	IP-адреса или диапазон IP-адресов, которые необходимо включить в список. Указывается в формате: <ip>, <ip/mask> или <ip_range_start-ip_range_end>.
use-in-search-queries	Должен ли использоваться данный список в поисковых запросах: • on; • off.

Для редактирования списка (список параметров, доступных для обновления, аналогичен списку параметров команды создания списка):
Admin@nodename# set libraries ip-list <ip-list-name> <parameters>
Чтобы добавить в список новые адреса:
Admin@nodename# set libraries ip-list <ip-list-name> [<ip1> <ip2> ...]
Следующие команды используются для удаления всего списка адресов или IP-адресов, содержащихся в нём:
Admin@nodename# delete libraries ip-list <ip-list-name>

```
Admin@nodename# delete libraries ip-list <ip-list-name> ips [ <ip1> <ip2>... ]
```

Команда отображения информации о всех имеющихся списках:

```
Admin@nodename# show libraries ip-list
```

Чтобы отобразить информацию об определённом списке, необходимо указать название интересующего списка IP-адресов:

```
Admin@nodename# show libraries ip-list <ip-list-name>
```

Также доступен просмотр содержимого списка IP-адресов:

```
Admin@nodename# show libraries ip-list <ip-list-name> items
```

Настройка useragent браузеров

Данный раздел находится на уровне **libraries useragents**. (Доступно начиная с релиза ПО 7.2.0).

Для создания списка useragent браузеров используется следующая команда:

```
Admin@nodename# create libraries useragents <parameters>
```

Далее необходимо задать следующие параметры:

Параметр	Описание
name	Название списка.
description	Описание списка.
patterns	Строка описания useragent. Исчерпывающий список строк aseragent представлен на этом ресурсе: http://www.useragentstring.com/pages/useragentstring.php .
type	Тип списка: • local — локальный. • updatable — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (url). Периодичность обновления списка указывается параметром shedule в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*" / 2 в поле "часы" будет означать "каждые два часа".
use-in-search-queries	Должен ли использоваться данный список в поисковых запросах: • on; • off.

Для редактирования списка (список параметров, доступных для обновления, аналогичен списку параметров команды создания списка):

```
Admin@nodename# set libraries useragents <list-name> <parameters>
```

Следующие команды используются для удаления всего списка или отдельных useragent из списка по их паттернам:

```
Admin@nodename# delete libraries useragents <list-name>
```

```
Admin@nodename# delete libraries useragents <list-name> <patterns>
```

Команда отображения информации о всех имеющихся списках:

```
Admin@nodename# show libraries useragents
```

Чтобы отобразить информацию об определённом списке, необходимо указать название интересующего списка:

```
Admin@nodename# show libraries useragents <list-name>
```

Также доступен просмотр содержимого конкретного списка useragents:

```
Admin@nodename# show libraries useragents <list-name> patterns
```

Настройка типов контента

Данный раздел находится на уровне **libraries content-types**. (Доступно начиная с релиза ПО 7.2.0).

Для создания списка типов контента используется следующая команда:

```
Admin@nodename# create libraries content-types <parameters>
```

Далее необходимо задать следующие параметры:

Параметр	Описание
name	Название списка.
description	Описание списка.
mime	Данные в формате MIME. Различные типы контента и их описание доступны по ссылке https://www.iana.org/assignments/media-types/media-types.xhtml .
type	Тип списка: • local — локальный. • updatable — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (url). Периодичность обновления списка указывается параметром shedule в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*" / 2 в поле "часы" будет означать "каждые два часа".
use-in-search-queries	Должен ли использоваться данный список в поисковых запросах: • on; • off.

Для редактирования списка (список параметров, доступных для обновления, аналогичен списку параметров команды создания списка):

```
Admin@nodename# set libraries content-types <list-name> <parameters>
```

Следующие команды используются для удаления всего списка или отдельных типов контента, содержащихся в нём:

```
Admin@nodename# delete libraries content-types <list-name>
```

```
Admin@nodename# delete libraries content-types <list-name> mime [ <mime1> <mime2>... ]
```

Команда отображения информации о всех имеющихся списках:

```
Admin@nodename# show libraries content-types
```

Чтобы отобразить информацию об определённом списке, необходимо указать название интересующего списка:

```
Admin@nodename# show libraries content-types <list-name>
```

Также доступен просмотр содержимого списка типов контента:

```
Admin@nodename# show libraries content-types <list-name> mime
```

Настройка списков URL

Данный раздел находится на уровне **libraries url-list**. (Доступно начиная с релиза ПО 7.2.0).

Для создания списка URL-адресов используется следующая команда:

```
Admin@nodename# create libraries url-list <parameters>
```

Далее необходимо задать следующие параметры:

Параметр	Описание
name	Название списка.
description	Описание списка.
case-sensitivity	Чувствительность к регистру в написании адреса URL: • sensitive — чувствительно к регистру букв в адресе. • insensitive — нечувствительно к регистру букв в адресе. • domain — список адресов доменов.
urls	URL, которые необходимо добавить в список.
type	Тип списка: • local — локальный. • updatable — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (url). Периодичность обновления списка указывается параметром shedule в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".
use-in-search-queries	Должен ли использоваться данный список в поисковых запросах: • on; • off.

Для редактирования списка (список параметров, доступных для обновления, аналогичен списку параметров команды создания списка):

Admin@nodename# set libraries url-list <list-name> <parameters>

Следующие команды используются для удаления всего списка или отдельных URL-адресов, содержащихся в нём:

Admin@nodename# delete libraries url-list <list-name>
Admin@nodename# delete libraries url-list <list-name> urls [<url1> <url2>...]

Команда отображения информации о всех имеющихся списках:

Admin@nodename# show libraries url-list

Чтобы отобразить информацию об определённом списке, необходимо указать название интересующего списка:

Admin@nodename# show libraries url-list <list-name>

Также доступен просмотр содержимого списка URL-адресов:

Admin@nodename# show libraries url-list <list-name> urls

Настройка почтовых адресов

Раздел находится на уровне **libraries email-list**.

Чтобы добавить новую группу почтовых адресов используется следующая команда:

Admin@nodename#& create libraries email-list <parameter>

Далее указываются параметры:

Параметр	Описание

Параметр	Описание
type	Тип списка: • local — локальный. • updatable — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (url). Периодичность обновления списка указывается параметром schedule в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".
phones	Номера телефонов, которые необходимо добавить в данную группу.

Для редактирования информации о группе телефонных номеров используется команда:

```
Admin@nodename# set libraries phone-list <phone-list-name> <parameter>
```

Параметры, доступные для обновления, представлены в таблице выше.

Для удаления группы или номеров телефонов из неё используются следующие команды:

```
Admin@nodename# delete libraries phone-list <phone-list-name>
```

```
Admin@nodename# delete libraries phone-list <phone-list-name> phones [ <phone> ... ]
```

Следующие команды используются для просмотра информации о всех созданных группах:

```
Admin@nodename# show libraries phone-list
```

или об определённых группах телефонных номеров:

```
Admin@nodename# show libraries phone-list <phone-list-name>
```

Для просмотра номеров, содержащихся в группе, используется команда:

```
Admin@nodename# show libraries phone-list <phone-list-name> phones
```

Настройка команд

Данный раздел позволяет создавать группы команд, предназначенных для отправки на коннекторы.

Для создания списка команд используется команда:

```
Admin@nodename# create libraries commands-list name <command-list-name> type <local | updatable> commands new <command-string>
```

Для редактирования созданного ранее списка команд используется команда:

```
Admin@nodename# set libraries commands-list <command-list-name> commands <command-string>
```

Для просмотра созданного ранее списка команд используется команда:

```
Admin@nodename# show libraries commands-list <command-list-name>
```

Для удаления созданного ранее списка команд или отдельных команд из списка используется команда:

```
Admin@nodename# delete libraries commands-list <command-list-name>
```

```
Admin@nodename# delete libraries commands-list <command-list-name> commands <command-string>
```

Настройка профилей оповещений

Профили оповещений SMTP (по email) и SMPP (по SMS) настраиваются на уровне **libraries notification-profiles**.

Для добавления нового профиля оповещения SMTP:

```
Admin@nodename# create libraries notification-profiles smtp <parameter>
```

Далее необходимо указать:

Параметр	Описание
----------	----------

Параметр	Описание
name	Название профиля.
description	Описание профиля.
host	IP-адрес или FQDN сервера SMTP, который будет использоваться для отсылки почтовых сообщений.
port	Порт TCP, используемый сервером SMTP. Обычно для протокола SMTP используется порт 25, для SMTP с использованием SSL — 465. Уточните данное значение у администратора почтового сервера.
connection-security	Варианты безопасности отправки почты; возможны варианты: • none. • starttls. • ssl.
authentication	Включение/отключение авторизации при подключении к серверу SMTP: • on. • off.
login	Имя учётной записи для подключения к SMTP-серверу.
password	Пароль учётной записи для подключения к SMTP-серверу.

Для создания профиля оповещения по SMS (SMPP):

Admin@nodename# create libraries notification-profiles smpp <parameter>

Далее необходимо указать значения следующих параметров:

Параметр	Описание
name	Название профиля.
description	Описание профиля.
host	IP-адрес или FQDN сервера SMPP, который будет использоваться для отсылки SMS.
port	Порт TCP, который используется для подключения к серверу SMPP. Обычно для протокола SMPP используется порт 2775; при использовании SSL — 3550.
ssl	Включение/отключение шифрования SSL: • on. • off.
login	Имя учётной записи для подключения к SMPP-серверу.
password	Пароль учётной записи для подключения к SMPP-серверу.
phone-translation-rules	Правила трансляции телефонных номеров. Правила используются для соответствия требованиям провайдера. Например, если необходимо заменить все номера, начинающиеся на +7, на 8: Admin@nodename# set libraries notification-profiles smpp <profile-name> phone-translation-rules + [+7 8]

Параметр	Описание
source-ton	Тип номера (Type of Number) для источника сообщения: • 0 — Unknown (Неизвестный). • 1 — International (Международный). • 2 — National (Государственный). • 3 — Network Specific (Сетевой Специальный). • 4 — Subscriber Number (Номер абонента). • 5 — Alphanumeric (Алфавитно-цифровой). • 6 — Abbreviated (Сокращённый).
dest-ton	Тип номера (Type of Number) для адресата: • 0 — Unknown (Неизвестный). • 1 — International (Международный). • 2 — National (Государственный). • 3 — Network Specific (Сетевой Специальный). • 4 — Subscriber Number (Номер абонента). • 5 — Alphanumeric (Алфавитно-цифровой). • 6 — Abbreviated (Сокращённый).
source-npi	Индикатор схемы присвоения номеров (Numbering Plan Indicator) для источника: • 0 — Unknown. • 1 — ISDN/telephone numbering plan (E.163/E.164). • 3 — Data numbering plan (X.121). • 4 — Telex numbering plan (F.69). • 6 — Land Mobile (E.212). • 8 — National numbering plan. • 9 — Private numbering plan. • 10 —ERMES numbering plan (ETSI DE/PS 3 01-3). • 13 — Internet (IP). • 18 — WAP Client Id (to be defined by WAP Forum).
dest-npi	Индикатор схемы присвоения номеров (Numbering Plan Indicator) для адресата: • 0 — Unknown. • 1 — ISDN/telephone numbering plan (E.163/E.164). • 3 — Data numbering plan (X.121). • 4 — Telex numbering plan (F.69). • 6 — Land Mobile (E.212). • 8 — National numbering plan. • 9 — Private numbering plan. • 10 —ERMES numbering plan (ETSI DE/PS 3 01-3). • 13 — Internet (IP). • 18 — WAP Client Id (to be defined by WAP Forum).

Для редактирования профиля оповещения используется команда:

Admin@nodename# set libraries notification-profiles <smtp | smpp> <profile-name> <parameter>

Параметры профилей SMTP и SMPP, доступные для изменения, представлены в соответствующих таблицах выше.

Для удаления профиля:

```
Admin@nodename# delete libraries notification-profiles <smtp | smpp> <profile-name>
```

Также для профилей оповещений SMPP доступно удаление правил трансляции номеров:

```
Admin@nodename# delete libraries notification-profiles smpp <profile-name> phone-translation-rules [ phone1|phone2 ]
```

Следующие команды предназначены для отображения информации о всех имеющихся профилях оповещений:

```
Admin@nodename# show libraries notification-profiles
```

о всех профилях одного типа:

```
Admin@nodename# show libraries notification-profiles <smtp | smpp>
```

об определённом профиле оповещения:

```
Admin@nodename# show libraries notification-profiles <smtp | smpp> <profile-name>
```

Настройка категорий срабатывания

Элемент библиотеки **Категории срабатываний** позволяет создать категории, по которым можно группировать определенные срабатывания правил аналитики, применяемые к событиям. Более подробно о правилах аналитики смотрите в разделе [Аналитика](#). По умолчанию создаются категории:

- **Availability** — правила аналитики, определяющие инциденты, приводящие к ухудшению доступности информационных систем.
- **Performance** — правила аналитики, определяющие инциденты, приводящие к ухудшению производительности информационных систем.
- **Security** — правила аналитики, определяющие инциденты, приводящие к ухудшению безопасности информационных систем.

Для создания категорий срабатывания используется команда:

```
Admin@nodename# create libraries alert-categories name <category-name> key <category-key>
```

Для редактирования категорий срабатывания используется команда:

```
Admin@nodename# set libraries alert-categories name <category-name> key <category-key>
```

Для просмотра созданных ранее категорий срабатывания используется команда:

```
Admin@nodename# show libraries alert-categories name <category-name>
```

Для удаления созданных ранее категорий срабатывания используется команда:

```
Admin@nodename# delete libraries alert-categories name <category-name>
```

Настройка внешних сервисов обогащений

В данном элементе библиотеки представлены ресурсы, с помощью которых происходит дополнительный сбор информации об угрозах. С данных источников приходят фиды — структурированные проанализированные данные об IP-адресах и доменах, с которых происходит распространение вредоносных файлов, их сэмплы и хэши; списки фишинговых сайтов, почтовые адреса отправителей фишинговых писем; адреса, с которых происходит сканирование сетей с целью обнаружения уязвимостей; IP-адреса, с которых проводятся атаки типа брутфорс; сигнатуры для обнаружения вредоносного программного обеспечения. Подробнее о доступных сервисах читайте в разделе [Внешние сервисы обогащений](#) Руководства администратора SIEM.

Чтобы использовать сервисы обогащения их необходимо включить. Для использования некоторых сервисов обогащения необходимо прохождение регистрации и предоставление ключа доступа.

Для редактирования сервисов обогащений используется команда:

```
Admin@nodename# set libraries enrichment-services <service-name>
```

Для просмотра сервисов обогащений используется команда:

```
Admin@nodename# show libraries enrichment-services <service-name>
```

Настройка syslog-фильтров

Создание и настройка syslog-фильтров производится на уровне **libraries syslog-filters**.

Команда для создания syslog-фильтра:

```
Admin@nodename# create libraries syslog-filters <parameter>
```

Далее представлены параметры, которые необходимо указать:

Параметр	Описание
----------	----------

Параметр	Описание
name	Название фильтра.
description	Описание фильтра.
login-address	Строка для поиска IP-адреса пользователя в syslog-сообщении.
login-event	Строка для поиска события входа пользователя в syslog-сообщении.
login-username	Строка для поиска имени пользователя в syslog-сообщении.
logout-address	Строка для поиска IP-адреса пользователя в syslog-сообщении.
logout-event	Строка для поиска события выхода пользователя в syslog-сообщении.
logout-username	Строка для поиска имени пользователя в syslog-сообщении.

Следующая команда предназначена для редактирования информации о syslog-фильтре:

```
Admin@nodename# set libraries syslog-filters <filter-name> <parameter>
```

Параметры, доступные для обновления, аналогичны параметрам, указываемым при создании фильтра.

Чтобы отобразить информацию о syslog-фильтрах:

```
Admin@nodename# show libraries syslog-filters <filter-name>
```

Пользователь может удалить syslog-фильтр, используя следующую команду:

```
Admin@nodename# delete libraries syslog-filters <filter-name>
```

Настройка приложений syslog

Создание и настройка приложений syslog производится на уровне **libraries syslog-application**.

Команда для создания приложений syslog:

```
Admin@nodename# create libraries syslog-application <parameter>
```

Далее представлены параметры, которые необходимо указать:

Параметр	Описание
name	Название приложения.
description	Описание приложения.
app-name	Название приложения, отображаемое в журналах.

