Cisco ISE

?????????? ?? ?????????

Cisco Identity Services Engine (Cisco ISE) - централизованная платформа управления сетевым доступом, аутентификацией и авторизацией пользователей и устройств в корпоративной сети. Используется для реализации политик контроля доступа на основе идентичности при работе с проводными, беспроводными и VPN-подключениями, а также для интеграции с сетевым оборудованием и системами информационной безопасности.

В рамках задач информационной безопасности Cisco ISE является источником событий аутентификации и авторизации, административных действий и учёта сессий доступа. Эти события применяются для мониторинга доступа, анализа инцидентов и формирования аудита в системах класса SIEM.

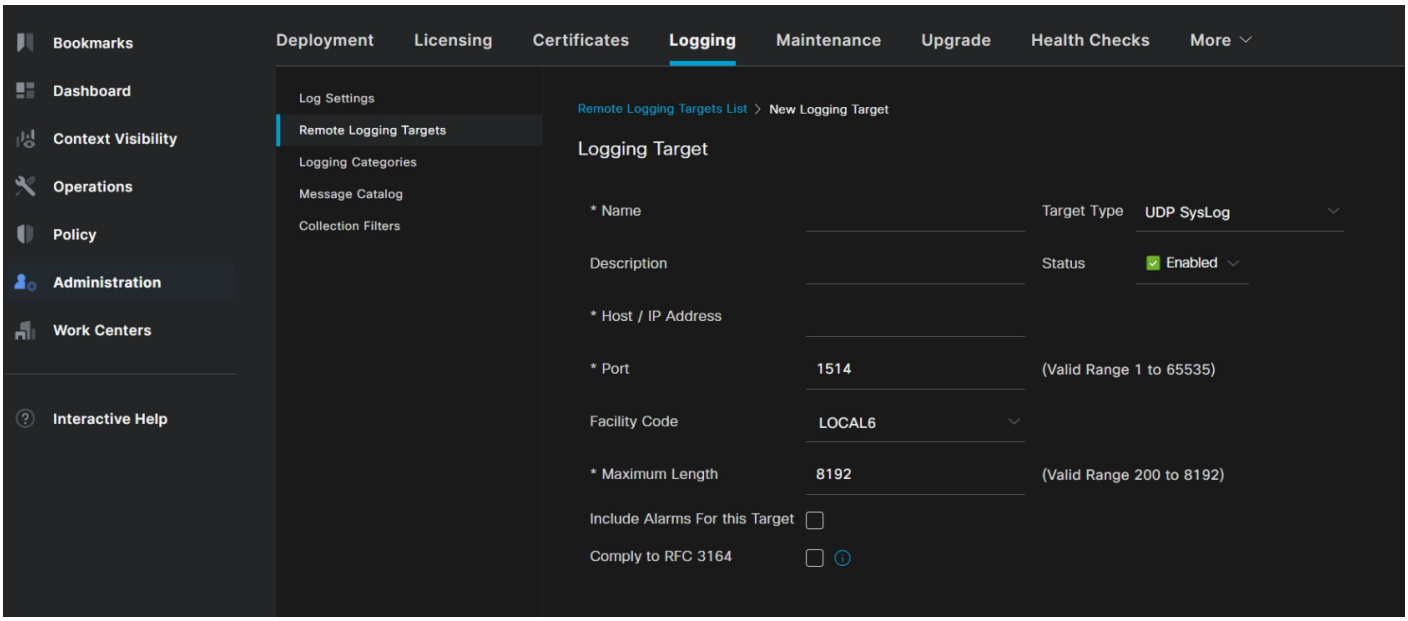
????????? ???????? ??????? Cisco ISE ?? ??????? SIEM ?? syslog

Подключение к интерфейсу управления:

1. В адресной строке браузера введите IP-адрес или доменное имя Cisco ISE.
2. Выполните вход под учетной записью, входящей в группу администраторов.

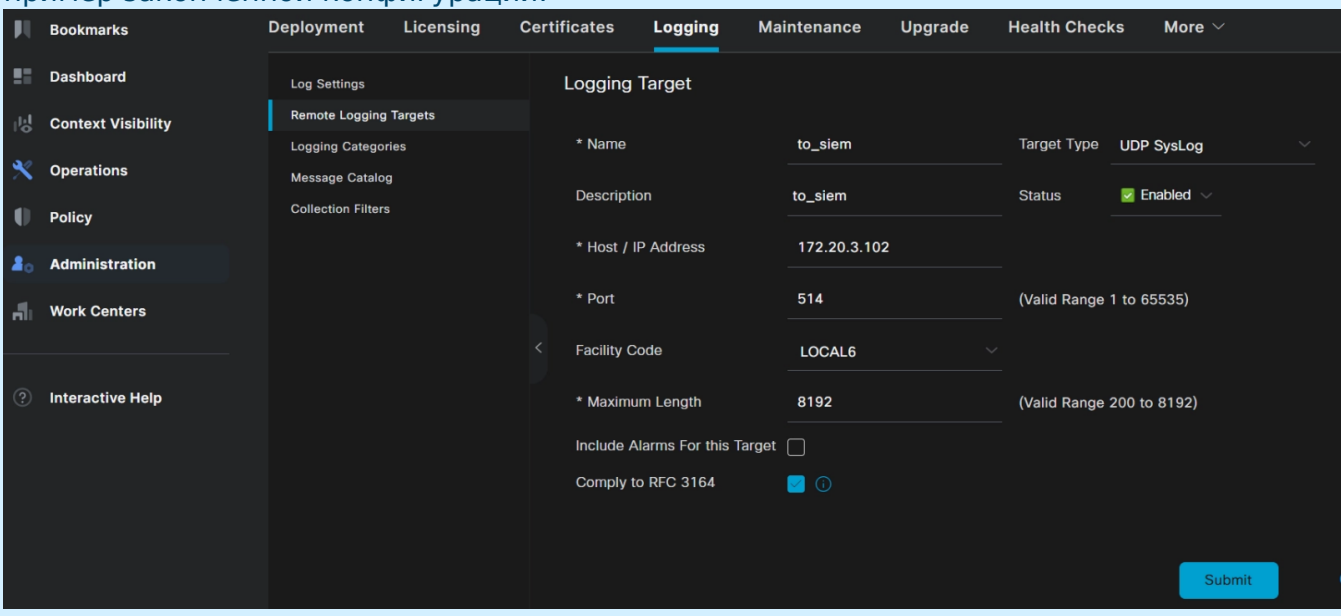
Создание профиля внешнего syslog-сервера:

1. В главном меню выберите **Administration → System → Logging**.
2. В левой части окна выберите **Remote Logging Targets**.
3. В панели инструментов нажмите кнопку **Add**.



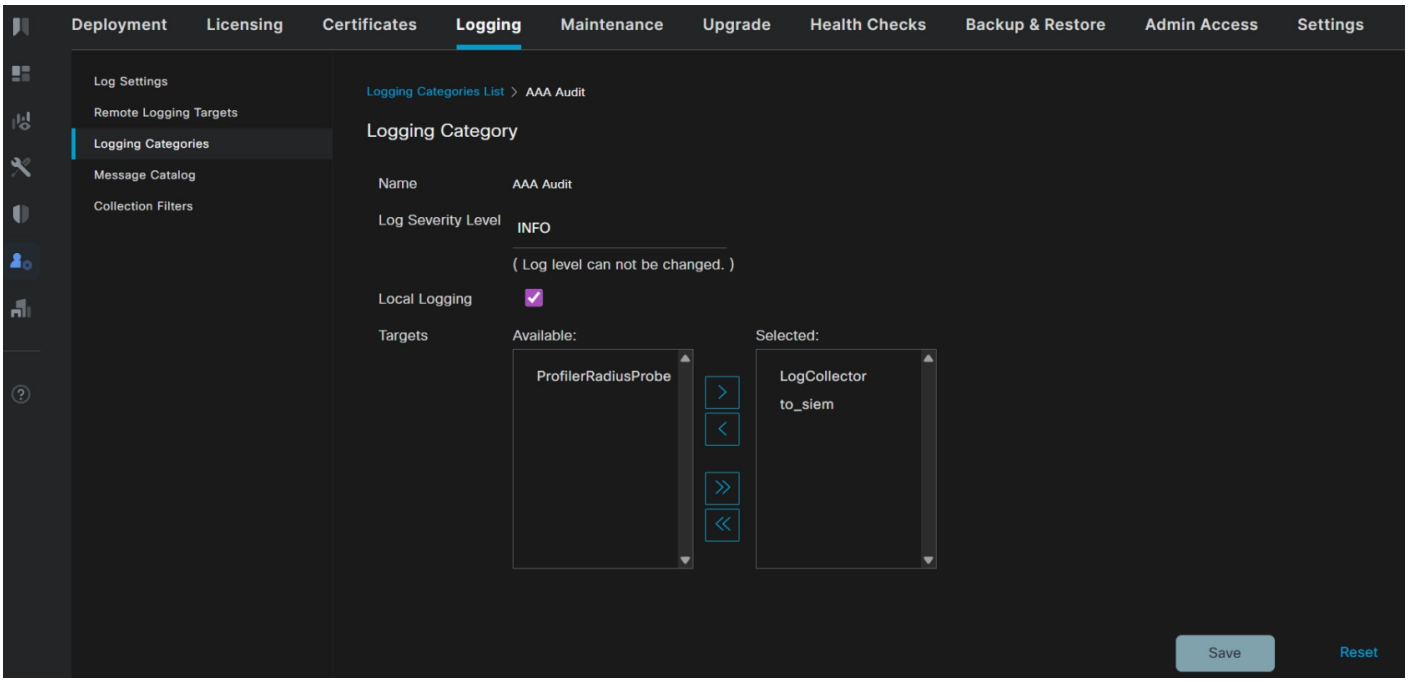
4. В поле **Name** укажите имя профиля внешнего syslog-сервера.
5. В поле **IP/Host Address** укажите IP-адрес или доменное имя сервера приёма syslog.
6. В поле **Port** укажите порт, используемый для приёма syslog-сообщений.
7. В поле **Target Type** выберите тип отправки (`UPD syslog` / `TCP syslog` / `Secure TCP`)
8. В поле **Facility Code** выберите facility (например, `LOCAL0`–`LOCAL7`) согласно принятой схеме на стороне SIEM
9. В поле **Maximum Length** укажите максимальную длину syslog-сообщения `8192`
10. **Comply to RFC 3164 -** Включите при необходимости, если SIEM ожидает формат сообщений по RFC 3164
11. Установите **Status = Enabled**
12. Нажмите кнопку **Submit**

пример законченной конфигурации:



???????? ???????? ?????????????

1. В левой части окна выберите **Logging Categories**.
2. Выберите категорию **AAA Audit** и в панели инструментов нажмите кнопку **Edit**.
3. В списке **Available** выберите созданный профиль syslog-сервера, в нашем случае **to_siem**.
4. Переместите выбранный профиль в список **Selected,** нажав на **>**.



????????? Severity ? Local Log

- **Severity -** Значение уровня важности событий используется по умолчанию и не требует изменений в рамках данной настройки.
- **Local Log -** Параметр локального журналирования остается без изменений и настраивается в соответствии с требованиями и особенностями текущей конфигурации Cisco ISE.

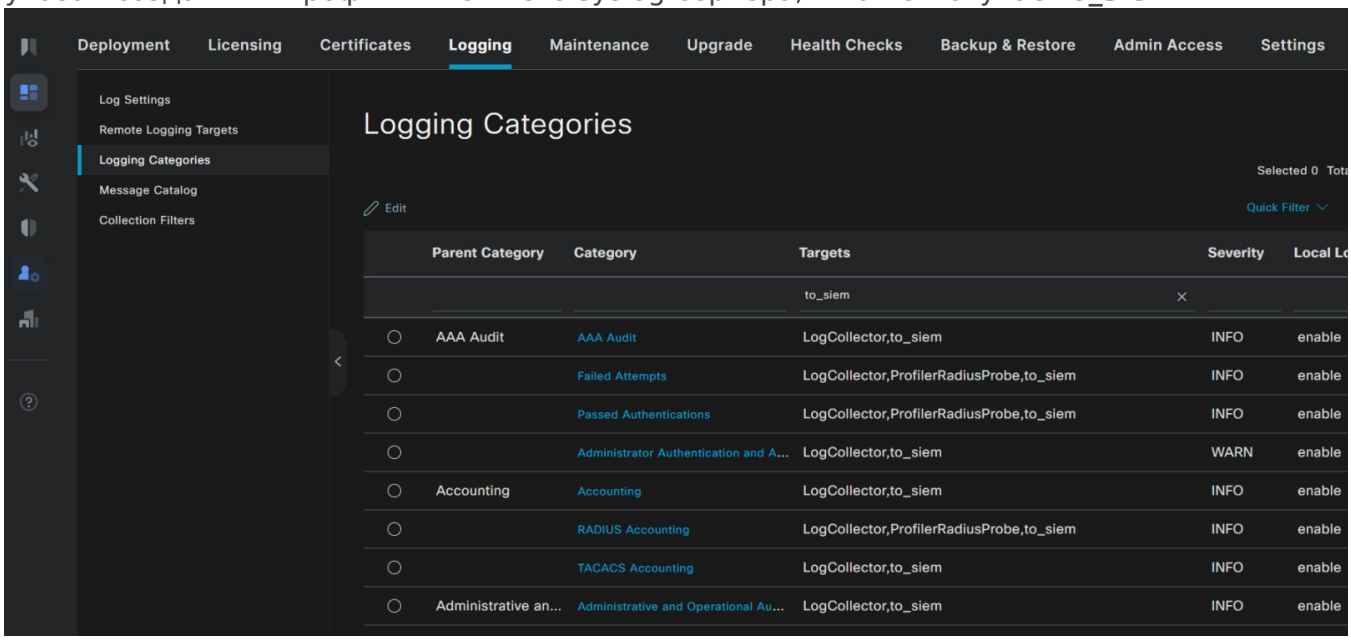
5. Нажмите кнопку **Save**.
6. Повторите шаги с **1 по 5** для следующих категорий событий:

- **Failed Attempts**
- **Passed Authentications**
- **Administrator Authentication and Authorization**
- **Accounting**
- **RADIUS Accounting**
- **TACACS Accounting**
- **Administrative and Operational Audit**

???????? ????????? ???????? ???????

1. В веб-интерфейсе Cisco ISE перейдите в раздел **Administration → System → Logging → Logging Categories**.
2. В списке категорий просмотрите колонку **Targets**.

3. Для ранее настроенных категорий событий убедитесь, что в колонке **Targets** указан созданный профиль внешнего syslog-сервера, в нашем случае **to_siem**.




```
Проверка выполняется для ранее настроенных категорий:

AAA Audit
Failed Attempts
Passed Authentications
Administrator Authentication and Authorization
Accounting
RADIUS Accounting
TACACS Accounting
Administrative and Operational Audit

Если для указанных категорий в колонке Targets отображается созданный профиль, в нашем случае
to_siem, настройка выполнена корректно, и события будут отправляться во внешнюю систему SIEM
```

После выполнения указанных шагов Cisco ISE начинает отправлять выбранные категории событий во внешнюю систему SIEM по протоколу syslog

---

Revision #2
Created 2026-05-25 10:31:59 UTC by lerat
Updated 2026-05-25 10:38:00 UTC by lerat