

Catalyst сеанс коммутатора серии 3850 осведомленные сети с сервисным шаблоном на примере конфигурации ISE

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Общие сведения](#)

[Настройка](#)

[Схема сети](#)

[Локально определенный сервисный шаблон](#)

[Сервисный шаблон, определенный на ISE](#)

[Конфигурация ISE](#)

[Catalyst конфигурация коммутатора серии 3850](#)

[Проверка](#)

[Локально определенный сервисный шаблон](#)

[Сервисный шаблон, определенный на ISE](#)

[Устранение неполадок](#)

[Локально определенный сервисный шаблон](#)

[Сервисный шаблон, определенный на ISE](#)

[Дополнительные сведения](#)

Введение

Этот документ описывает, как настроить идентификационные сервисы на Cisco Catalyst коммутатор серии 3850 с Сеансом Осведомленная Сетевая платформа. Это - новый способ настроить идентификационные сервисы (802.1x, Обход проверки подлинности MAC (MAB), WebAuth), который обеспечивает большую гибкость и функциональность. Это использует Язык Политики Общей классификации Cisco (C3PL) наряду с сервисными шаблонами, которые могут быть сохранены локально или на платформе Cisco Identity Services Engine (ISE) сервер.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Catalyst коммутатор серии 3850, Cisco IOS® CLI
- Cisco ISE
- Идентификационные Сервисы (802.1x/MAB/WebAuth)

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Catalyst Коммутатор серии 3850, версия Cisco IOS 03.03.00SE или позже
- Версия 1.2 Cisco ISE или позже

Примечание: См. [руководство по развертыванию IBNS 2.0](#) для просмотра матрицы поддержки.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Общие сведения

Сервисные шаблоны содержат ряд атрибутов политики, которые могут быть присоединены к пользовательскому сеансу через определенное действие в политике контроля. Два примера представлены в этом документе:

- MAB и локально определенный сервисный шаблон используются для сценария отказов.
- MAB и шаблон определенного сервиса ISE используются для сценария отказов.

MAB используется в качестве примера в этом документе. Однако возможно использовать 802.1x и/или WebAuth и политику комплекса сборки с C3PL.

Настройка

Примечание: [Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд \(только для зарегистрированных клиентов\).](#)

Схема сети

Оба примера, представленные здесь, включают Компьютер с операционной системой Windows, который соединяется с коммутатором, который выполняет MAB. Windows MAC address не настроен на ISE, который является, почему отказывает MAB. Затем коммутатор применяет политику, определенную в сервисном шаблоне.

Локально определенный сервисный шаблон

После сбоя MAB коммутатор применяет локально определенный сервисный шаблон.

Вот поток:

1. Windows передает Фрейм Ethernet.
2. Коммутатор выполняет MAB и передает RADIUS-Request к ISE с MAC-адресом как имя пользователя.
3. ISE не настроили ту конечную точку и возвращает Отклонение RADIUS.
4. Коммутатор активирует локально определенную политику шаблона MAB_FAIL.

Для большего количества полной информации обратитесь к [Основанному на идентичности Руководству по конфигурации Сетевых сервисов, Выпуск 3SE Cisco IOS XE \(Коммутаторы Catalyst 3850\)](#).

Вот базовый пример:

```
aaa new-model
!
aaa group server radius ISE
  server name ISE
!
aaa authentication dot1x default group ISE
aaa authorization network default group ISE
aaa accounting identity default start-stop group ISE

dot1x system-auth-control

service-template MAB_FAIL_LOCAL <--- Local service template
  access-group MAB_FAIL_LOCAL_ACL

class-map type control subscriber match-all MAB-FAIL
  match result-type method mab authoritative <--- class MAB failure
!
policy-map type control subscriber POLICY_MAB
  event session-started match-all
  10 class always do-until-failure
    10 authenticate using mab aaa authc-list ISE priority 20 <--- try MAB
    20 authenticate using mab aaa authz-list ISE priority 20
  event authentication-failure match-first
  10 class MAB-FAIL do-until-failure
    20 activate service-template MAB_FAIL_LOCAL <--- apply local template service
for the MAB failure

interface GigabitEthernet1/0/1
  switchport mode access
  access-session port-control auto
  mab
  spanning-tree portfast
  service-policy type control subscriber POLICY_MAB

radius server ISE
  address ipv4 10.48.66.74 auth-port 1645 acct-port 1646
  key cisco
```

```
ip access-list extended MAB_FAIL_LOCAL_ACL
permit icmp any any
```

Сервисный шаблон, определенный на ISE

Вот поток:

1. Windows передает Фрейм Ethernet.
2. Коммутатор выполняет MAB и передает RADIUS-Request к ISE с MAC-адресом как имя пользователя.
3. ISE не настроили ту конечную точку и возвращает Отклонение RADIUS.
4. Коммутатор активирует политику шаблона **MAB_FAIL** с Аутентификацией, авторизацией и учетом (AAA) ISE - список. RADIUS-Request передается с именем пользователя как имя шаблона (**MAB_FAIL**) и жестко закодированный пароль: **cisco123**. Кроме того, Пара Значения атрибута (AV) Cisco подключена **download-request=service-template**.
5. Та пара значение-атрибут вынуждает ISE рассматривать тот запрос, как сервис обрабатывают запрос по шаблону. Все проверки для правил проверки подлинности и авторизация опущены. ISE только проверяет, существует ли профиль авторизации с тем же названием (**MAB_FAIL**). Нет никакой потребности настроить пользователя **MAB_FAIL** в хранилище локального пользователя. Затем ISE возвращает все атрибуты, привязанные к тому профилю, который является Загружаемым списком контроля доступа (DACL) в данном примере.
6. Если DACL не кэшируется на коммутаторе, он передает другой RADIUS-Request за тем DACL.
7. Содержание DACL возвращено. Коммутатор применяет политику.

Конфигурация ISE

После добавления Устройства Доступа к сети Профиль Авторизации требуется:

Важно проверить флажок **Service Template** и использовать то же название в качестве того, определенного на коммутаторе.

Catalyst конфигурация коммутатора серии 3850

Эта конфигурация имеет четыре различия от первого примера:

- Локальный шаблон политики **MAB_FAIL_LOCAL** удален.
- Поддержка изменения авторизации (CoA) добавлена.

- Список ISE для шаблона политики **MAB_FAIL** (политика, настроенная на ISE), используется.
- AAA authorization list для сервисного извлечения шаблона называют.

Вот настройка:

```

aaa new-model
!
aaa group server radius ISE
  server name ISE
!
aaa authentication dot1x default group ISE
aaa authorization network default group ISE
aaa authorization network ISE group ISE <--- used to retrieve
service-template
from ISE
aaa accounting identity default start-stop group ISE

dot1x system-auth-control

aaa server radius dynamic-author
  client 10.48.66.74 server-key cisco

class-map type control subscriber match-all MAB-FAIL
  match result-type method mab authoritative <--- class MAB failure
!
policy-map type control subscriber POLICY_MAB
  event session-started match-all
  10 class always do-until-failure
    10 authenticate using mab aaa authc-list ISE priority 20 <--- try MAB
    20 authenticate using mab aaa authz-list ISE priority 20
  event authentication-failure match-first
  10 class MAB-FAIL do-until-failure
    20 activate service-template MAB_FAIL aaa-list ISE replace-all <--- apply
template
policy defined on ISE for the MAB failure

interface GigabitEthernet1/0/1
  switchport mode access
  access-session port-control auto
  mab
  spanning-tree portfast
  service-policy type control subscriber POLICY_MAB

radius server ISE
  address ipv4 10.48.66.74 auth-port 1645 acct-port 1646
  key cisco

```

Необходимо настроить поддержку RADIUS CoA на коммутаторе после изменения шаблона (профиль авторизации) на ISE потому что это передает CoA для обновления шаблона на коммутаторе.

Проверка

Локально определенный сервисный шаблон

На Catalyst коммутатор серии 3850 введите эту команду для проверки пользовательского

сеанса:

```
3850-1#show access-session int g1/0/1 details
  Interface: GigabitEthernet1/0/1
    IIF-ID: 0x1091E80000000B0
  MAC Address: dc7b.94a3.7005
  IPv6 Address: Unknown
  IPv4 Address: Unknown
  User-Name: dc7b94a37005
  Status: Unauthorized
  Domain: DATA
  Oper host mode: multi-auth
  Oper control dir: both
  Session timeout: N/A
  Common Session ID: 0A30276F0000117D52D8816C
  Acct Session ID: Unknown

  Handle: 0x50000368
  Current Policy: POLICY_MAB
```

```
Local Policies:
  Template: MAB_FAIL_LOCAL (priority 150)
  Filter-ID: MAB_FAIL_LOCAL_ACL
```

```
Method status list:
  Method      State
  mab         Authc Failed
```

```
3850-1#sh ip access-lists MAB_FAIL_LOCAL_ACL
Extended IP access list MAB_FAIL_LOCAL_ACL
  10 permit icmp any any
```

Сервисный шаблон, определенный на ISE

На Catalyst коммутатор серии 3850 введите эту команду для проверки пользовательского сеанса:

```
3850-1# show access-session interface g1/0/1 details
  Interface: GigabitEthernet1/0/1
    IIF-ID: 0x1058A40000000AB
  MAC Address: dc7b.94a3.7005
  IPv6 Address: Unknown
  IPv4 Address: Unknown
  User-Name: dc7b94a37005
  Status: Unauthorized
  Domain: DATA
  Oper host mode: multi-auth
  Oper control dir: both
  Session timeout: N/A
  Common Session ID: 0A30276F0000116851173EFE
  Acct Session ID: Unknown
  Handle: 0xCC000363
  Current Policy: POLICY_MAB
```

```
Local Policies:
  Template: MAB_FAIL (priority 150)
  ACS ACL: xACSACLx-IP-MAB-FAIL-ACL-528741f3
```

```
Method status list:
  Method      State
  mab         Authc Failed
```

Обратите внимание на то, что состояние **Подведено**, но что применены определенный шаблон и связанный DACL:

```
3850-1#show ip access-lists
Extended IP access list implicit_deny_acl
 10 deny ip any any
Extended IP access list xACSACLx-IP-MAB-FAIL-ACL-528741f3 (per-user)
 1 permit icmp any any <--- DACL from ISE
```

Список контроля доступа (ACL) не видим под интерфейсом:

```
3850-1#show ip access-lists interface g1/0/1 in
3850-1#show ip access-lists interface g1/0/1
3850-1#show ip access-lists interface g1/0/1 out
3850-1#
```

Возможно проверить, запрограммирован ли ASIC (аппаратные средства) правильно:

```
3850-1# show platform acl
#####
#####
#####      Printing LE Infos      #####
#####
#####
#####
#####
## LE INFO: (LETYPE: Group)
#####
LE: 7 (Client MAC dc7b.94a3.7005) (ASIC1)
-----
leinfo: 0x5171eea0
LE handle: 0x61120fb0
LE Type: Group
IIF ID: 0x1058a40000000ab
Input IPv4 ACL: label 4 h/w 4 (read from h/w 4)
  BO 0x196000000 [CGACL]: xACSACLx-IP-MAB-FAIL-ACL-528741f3
  BO 0x1fffffa00 [CGACL]: implicit_deny_acl
Output IPv4 ACL: label 0 h/w 0 (Group LE and label are not linked)
Input IPv6 ACL: label 0 h/w 0 (Group LE and label are not linked)
Output IPv6 ACL: label 0 h/w 0 (Group LE and label are not linked)
Input MAC ACL: label 0 h/w 0 (Group LE and label are not linked)
Output MAC ACL: label 0 h/w 0 (Group LE and label are not linked)
```

Каждому пользовательскому сеансу, который имеет другой DACL, запрограммирую отдельную запись в ASIC. На ISE существует три отдельных аутентификации:

- Отказавший MAB
- Успешное сервисное извлечение шаблона (MAB_FAIL)
- Успешное извлечение DACL

Вот более внимательное рассмотрение при шагах при получении запроса о сервисном шаблоне:

- 11001 Полученный Access-Request RADIUS
- 11017 RADIUS создал новый сеанс
- 11022 Добавленный DACL задан в Профиле Авторизации
- 11002 Возвращенный Access-Accept RADIUS

Это ясно показывает, что не обработана Аутентификация/Правила авторизации.

Устранение неполадок

Локально определенный сервисный шаблон

Вот отладки для текущего сценария. Некоторые выходные данные опущены для ясности:

```
3850-1#show debugging
```

```
epm:
```

```
EPM session error debugging is on
EPM session error detailed debugging is on
EPM fsm error debugging is on
EPM fsm error detailed debugging is on
EPM packet error debugging is on
EPM packet error detailed debugging is on
EPM SPI errors debugging is on
EPM session events debugging is on
EPM fsm events debugging is on
EPM fsm events detailed debugging is on
EPM packet events debugging is on
EPM packet events detailed debugging is on
EPM SPI events debugging is on
```

```
Radius protocol debugging is on
Radius protocol verbose debugging is on
Radius packet protocol debugging is on
```

```
Auth Manager:
```

```
Auth Manager errors debugging is on
Auth Manager events debugging is on
Auth Manager detailed debugs debugging is on
Auth Manager sync debugging is on
```

```
dot1x:
```

```
Dot1x registry info debugging is on
Dot1x redundancy info debugging is on
Dot1x packet info debugging is on
Dot1x events debugging is on
Dot1x State machine transitions and actions debugging is on
Dot1x Errors debugging is on
Dot1x Supplicant EAP-FAST debugging is on
Dot1x Manager debugging is on
Dot1x Supplicant State Machine debugging is on
```

```
*Nov 16 11:45:10.680: AUTH-EVENT: [dc7b.94a3.7005, Gil/0/1] New client
dc7b.94a3.7005 - client handle 0x00000001 for SVM
*Nov 16 11:45:11.347: AUTH-DETAIL: [dc7b.94a3.7005, Gil/0/1] Create attr list,
session 0x50000368:
*Nov 16 11:45:11.347: AUTH-DETAIL: [dc7b.94a3.7005, Gil/0/1] - adding MAC
dc7b.94a3.7005
*Nov 16 11:45:11.347: AUTH-DETAIL: [dc7b.94a3.7005, Gil/0/1] - adding Swidb
0x38A8DABC
*Nov 16 11:45:11.348: AUTH-DETAIL: [dc7b.94a3.7005, Gil/0/1] - adding
AAA_ID=117D
*Nov 16 11:45:11.348: AUTH-DETAIL: [dc7b.94a3.7005, Gil/0/1] - adding
Audit_sid=0A30276F0000117D52D8816C
*Nov 16 11:45:11.348: AUTH-DETAIL: [dc7b.94a3.7005, Gil/0/1] - adding IIF
ID=0x1091E80000000B0
*Nov 16 11:45:11.348: AUTH-EVENT: [dc7b.94a3.7005, Gil/0/1] Policy processing
started for 0x50000368(dc7b.94a3.7005)
*Nov 16 11:45:11.348: AUTH-EVENT: [dc7b.94a3.7005, Gil/0/1] Policy event will
be processed synchronously for 0x50000368
```



```

*Nov 16 11:45:11.348: AUTH-EVENT: [dc7b.94a3.7005, Gi1/0/1] Processing default
action(s) for event SESSION_STARTED for session 0x50000368
*Nov 16 11:45:11.354: RADIUS/ENCODE: Best Local IP-Address 10.48.39.111 for
Radius-Server 10.48.66.74
*Nov 16 11:45:11.354: RADIUS(00000000): Send Access-Request to 10.48.66.74:1645
id 1645/2, len 260
*Nov 16 11:45:11.354: RADIUS: authenticator 86 FC 11 6A 6E 8D A1 0B - A6 98
8B 80 A2 DD A9 69
*Nov 16 11:45:11.354: RADIUS: User-Name [1] 14 "dc7b94a37005"
*Nov 16 11:45:11.354: RADIUS: User-Password [2] 18 *
*Nov 16 11:45:11.354: RADIUS: Service-Type [6] 6 Call Check [10]
*Nov 16 11:45:11.354: RADIUS: Vendor, Cisco [26] 31
*Nov 16 11:45:11.354: RADIUS: Cisco AVpair [1] 25 "service-type=Call Check"
*Nov 16 11:45:11.354: RADIUS: Framed-MTU [12] 6 1500
*Nov 16 11:45:11.354: RADIUS: Called-Station-Id [30] 19 "68-BC-0C-5A-61-01"
*Nov 16 11:45:11.354: RADIUS: Calling-Station-Id [31] 19 "DC-7B-94-A3-70-05"
*Nov 16 11:45:11.354: RADIUS: Message-Authenticato[80] 18
*Nov 16 11:45:11.354: RADIUS: 2D 20 38 B1 DF B6 C1 0C 0D AA 1D 9D E4 3E C8 0B [ - 8>]
*Nov 16 11:45:11.354: RADIUS: EAP-Key-Name [102] 2 *
*Nov 16 11:45:11.354: RADIUS: Vendor, Cisco [26] 49
*Nov 16 11:45:11.354: RADIUS: Cisco AVpair [1] 43 "audit-session-id=
0A30276F0000117D52D8816C"
*Nov 16 11:45:11.355: RADIUS: Vendor, Cisco [26] 18
*Nov 16 11:45:11.355: RADIUS: Cisco AVpair [1] 12 "method=mab"
*Nov 16 11:45:11.355: RADIUS: NAS-IP-Address [4] 6 10.48.39.111
*Nov 16 11:45:11.355: RADIUS: NAS-Port [5] 6 60000
*Nov 16 11:45:11.355: RADIUS: NAS-Port-Id [87] 22 "GigabitEthernet1/0/1"
*Nov 16 11:45:11.355: RADIUS: NAS-Port-Type [61] 6 Ethernet [15]
*Nov 16 11:45:11.355: RADIUS(00000000): Sending a IPv4 Radius Packet
*Nov 16 11:45:11.355: RADIUS(00000000): Started 5 sec timeout
*Nov 16 11:45:12.008: RADIUS: Received from id 1645/2 10.48.66.74:1645, Access-Reject,
len 38
*Nov 16 11:45:12.009: RADIUS: authenticator 9D 52 F8 CF 31 46 5A 17 - 4C 45 7E 89 9F
E2 2A 84
*Nov 16 11:45:12.009: RADIUS: Message-Authenticato[80] 18
*Nov 16 11:45:12.009: RADIUS: 11 F4 99 84 9B CC 7C 61 C7 75 7E 70 87 EC 64 8D [ |au~pd]
*Nov 16 11:45:12.009: RADIUS(00000000): Received from id 1645/2
*Nov 16 11:45:12.012: %MAB-5-FAIL: Authentication failed for client (dc7b.94a3.7005)
on Interface Gi1/0/1 AuditSessionID 0A30276F0000117D52D8816C
*Nov 16 11:45:12.013: AUTH-EVENT: [dc7b.94a3.7005, Gi1/0/1] Client dc7b.94a3.7005,
Method mab changing state from 'Running' to 'Authc Failed'
*Nov 16 11:45:12.013: AUTH-EVENT: Raised event RX_METHOD_AUTHC_FAIL (6) on handle
0x50000368
*Nov 16 11:45:12.016: EPM_SESS_EVENT: Feature (EPM ACL PLUG-IN) has been
started (status 2)
*Nov 16 11:45:12.016: %EPM-6-POLICY_REQ: IP 0.0.0.0| MAC dc7b.94a3.7005| AuditSessionID
0A30276F0000117D52D8816C| EVENT APPLY
*Nov 16 11:45:12.016: %EPM-6-POLICY_APP_SUCCESS: Policy Application succeeded for Client
[0.0.0.0] MAC [dc7b.94a3.7005] AuditSession ID [0A30276F0000117D52D8816C] for POLICY_TYPE
[Filter ID] POLICY_NAME [MAB_FAIL_LOCAL_ACL]

```

Сервисный шаблон, определенный на ISE

Вот отладки для текущего сценария. Некоторые выходные данные опущены для ясности:

<debug command omitted for clarity>

```

*Nov 16 03:34:28.670: AUTH-EVENT: [dc7b.94a3.7005, Gi1/0/1] Processing default
action(s) for event SESSION_STARTED for session 0xCC000363.
*Nov 16 03:34:28.679: RADIUS(00000000): Send Access-Request to 10.48.66.74:1645
id 1645/249, len 260
*Nov 16 03:34:28.679: RADIUS: authenticator CE 06 B0 C4 84 1D 70 82 - B8 66 2F

```

27 92 73 B7 E7

*Nov 16 03:34:28.679: RADIUS: **User-Name** [1] 14 "dc7b94a37005"

...

*Nov 16 03:34:29.333: RADIUS: **Received from id 1645/249 10.48.66.74:1645, Access-Reject,**
len 38

...

*Nov 16 03:34:29.335: %MAB-5-FAIL: Authentication failed for client (dc7b.94a3.7005)
on Interface Gi1/0/1 AuditSessionID 0A30276F0000116851173EFE

*Nov 16 03:34:29.336: AUTH-EVENT: [dc7b.94a3.7005, Gi1/0/1] **Authc failure** from MAB (2),
status Cred Fail (1) / event fail (1)

*Nov 16 03:34:29.339: %EPM-6-AAA: **POLICY MAB_FAIL| EVENT DOWNLOAD_REQUEST**

*Nov 16 03:34:29.340: EPM_SESS_EVENT: Method list used for download is ISE

*Nov 16 03:34:29.340: RADIUS(00000000): **Send Access-Request to 10.48.66.74:1645 id 1645/250,**
len 113

*Nov 16 03:34:29.340: RADIUS: authenticator B8 37 70 B0 33 F4 F2 FD - E4 C6 36
2A 4D BD 34 30

*Nov 16 03:34:29.341: RADIUS: NAS-IP-Address [4] 6 10.48.39.111

*Nov 16 03:34:29.341: RADIUS: **User-Name** [1] 10 "MAB_FAIL"

*Nov 16 03:34:29.341: RADIUS: User-Password [2] 18 *

*Nov 16 03:34:29.341: RADIUS: Vendor, Cisco [26] 41

*Nov 16 03:34:29.341: RADIUS: **Cisco AVpair** [1] 35 "download-request=
service-template"

*Nov 16 03:34:29.341: RADIUS: Message-Authenticato[80] 18

*Nov 16 03:34:29.341: RADIUS: EF D6 81 F7 5E 03 10 3B 91 EE 36 6E 9D 04
5B F4 [^;6n[]

*Nov 16 03:34:29.341: RADIUS(00000000): Sending a IPv4 Radius Packet

*Nov 16 03:34:29.341: RADIUS(00000000): Started 5 sec timeout

*Nov 16 03:34:29.342: EPM_SESS_EVENT: Received IPv4 Binding [ADD] Notification
[GigabitEthernet1/0/48 000c.29f3.ab14 10.48.39.131 1]

*Nov 16 03:34:29.342: EPM_SESS_EVENT: Received IPv4 Binding [ADD] Notification
[GigabitEthernet1/0/48 0050.5699.5350 10.48.39.211 1]

*Nov 16 03:34:29.867: RADIUS: **Received from id 1645/250 10.48.66.74:1645,**
Access-Accept, len 208

*Nov 16 03:34:29.867: RADIUS: authenticator A3 11 DA 4C 17 7E D3 86 - 06 78
85 5F 84 05 36 0B

*Nov 16 03:34:29.867: RADIUS: User-Name [1] 10 "MAB_FAIL"

*Nov 16 03:34:29.867: RADIUS: State [24] 40

*Nov 16 03:34:29.867: RADIUS: 52 65 61 75 74 68 53 65 73 73 69 6F 6E 3A
30 61 [ReauthSession:0a]

*Nov 16 03:34:29.867: RADIUS: 33 30 34 32 34 61 30 30 30 30 31 32 30 44
35 32 [30424a0000120D52]

*Nov 16 03:34:29.867: RADIUS: 38 37 34 38 32 45 [87482E]

*Nov 16 03:34:29.867: RADIUS: Class [25] 51

*Nov 16 03:34:29.867: RADIUS: 43 41 43 53 3A 30 61 33 30 34 32 34 61 30
30 30 [CACs:0a30424a000]

*Nov 16 03:34:29.868: RADIUS: 30 31 32 30 44 35 32 38 37 34 38 32 45 3A
69 73 [0120D5287482E:is]

*Nov 16 03:34:29.868: RADIUS: 65 32 2F 31 37 33 37 31 31 34 31 36 2F 35
30 30 [e2/173711416/500]

*Nov 16 03:34:29.868: RADIUS: 32 [2]

*Nov 16 03:34:29.868: RADIUS: Message-Authenticato[80] 18

*Nov 16 03:34:29.868: RADIUS: 1F 10 85 09 86 2C 5F 87 96 82 C8 3B 09 35 FD
96 [,_;5]

*Nov 16 03:34:29.868: RADIUS: Vendor, Cisco [26] 69

*Nov 16 03:34:29.868: RADIUS: **Cisco AVpair** [1] 63 "ACS:

CiscoSecure-Defined-ACL=#ACSACL#-IP-MAB-FAIL-ACL-528741f3"

*Nov 16 03:34:29.868: RADIUS(00000000): Received from id 1645/250

*Nov 16 03:34:29.869: %EPM-6-AAA: **POLICY MAB_FAIL| EVENT DOWNLOAD-SUCCESS**

*Nov 16 03:34:29.873: EPM_SESS_EVENT: Added method name ISE

*Nov 16 03:34:29.873: EPM_SESS_EVENT: Attribute CiscoSecure-Defined-ACL is
added to feat EPM ACL PLUG-IN list

*Nov 16 03:34:29.875: %EPM-6-POLICY_REQ: IP 0.0.0.0| MAC dc7b.94a3.7005|
AuditSessionID 0A30276F0000116851173EFE| EVENT APPLY

*Nov 16 03:34:29.875: %EPM-6-AAA: **POLICY xACSACLx-IP-MAB-FAIL-ACL-528741f3|**

EVENT DOWNLOAD_REQUEST

*Nov 16 03:34:29.876: RADIUS(00000000): **Send Access-Request to 10.48.66.74:1645**
id 1645/251, len 141
*Nov 16 03:34:29.876: RADIUS: authenticator BA 4C 97 06 E9 9E D5 03 - 1C 48
63 E6 94 D7 F8 DB
*Nov 16 03:34:29.876: RADIUS: NAS-IP-Address [4] 6 10.48.39.111
*Nov 16 03:34:29.876: RADIUS: **User-Name [1] 35 "#ACSACL#-IP-**

MAB-FAIL-ACL-528741f3"

*Nov 16 03:34:29.876: RADIUS: Vendor, Cisco [26] 32
*Nov 16 03:34:29.876: RADIUS: Cisco AVpair [1] 26 "aaa:service=
ip_admission"
*Nov 16 03:34:29.876: RADIUS: Vendor, Cisco [26] 30
*Nov 16 03:34:29.877: RADIUS: Cisco AVpair [1] 24 "aaa:event=

acl-download"

*Nov 16 03:34:29.877: RADIUS: Message-Authenticato[80] 18
*Nov 16 03:34:29.877: RADIUS: B1 4C E4 15 24 06 B4 1D E4 48 60 A0 9F 75
27 29 [L\$H`u')]
*Nov 16 03:34:29.877: RADIUS(00000000): Sending a IPv4 Radius Packet
*Nov 16 03:34:29.877: RADIUS(00000000): Started 5 sec timeout
*Nov 16 03:34:30.533: RADIUS: **Received from id 1645/251 10.48.66.74:1645,**
Access-Accept, len 202

*Nov 16 03:34:30.533: RADIUS: authenticator FA F9 55 1B 2A E2 32 0F - 33
C6 F9 FF BC C1 BB 7C

*Nov 16 03:34:30.533: RADIUS: User-Name [1] 35 "#ACSACL#-IP-
MAB-FAIL-ACL-528741f3"

*Nov 16 03:34:30.533: RADIUS: State [24] 40

*Nov 16 03:34:30.534: RADIUS: 52 65 61 75 74 68 53 65 73 73 69 6F 6E 3A
30 61 [ReauthSession:0a]

*Nov 16 03:34:30.534: RADIUS: 33 30 34 32 34 61 30 30 30 30 31 32 30 45
35 32 [30424a0000120E52]

*Nov 16 03:34:30.534: RADIUS: 38 37 34 38 32 45 [87482E]

*Nov 16 03:34:30.534: RADIUS: Class [25] 51

*Nov 16 03:34:30.534: RADIUS: 43 41 43 53 3A 30 61 33 30 34 32 34 61 30
30 30 [CACS:0a30424a000]

*Nov 16 03:34:30.534: RADIUS: 30 31 32 30 45 35 32 38 37 34 38 32 45 3A
69 73 [0120E5287482E:is]

*Nov 16 03:34:30.534: RADIUS: 65 32 2F 31 37 33 37 31 31 34 31 36 2F 35
30 30 [e2/173711416/500]

*Nov 16 03:34:30.534: RADIUS: 33 [3]

*Nov 16 03:34:30.534: RADIUS: Message-Authenticato[80] 18

*Nov 16 03:34:30.534: RADIUS: 96 9B AC 2C 28 47 25 B1 CF EA BD D0 7D F3
44 34 [,(G?}D4]

*Nov 16 03:34:30.534: RADIUS: Vendor, Cisco [26] 38

*Nov 16 03:34:30.534: RADIUS: Cisco AVpair [1] 32 "ip:inacl#1=

permit icmp any any"

*Nov 16 03:34:30.534: RADIUS(00000000): Received from id 1645/251

*Nov 16 03:34:30.535: %EPM-6-AAA: POLICY xACSACLx-IP-MAB-FAIL-ACL-528741f3|

EVENT DOWNLOAD-SUCCESS

*Nov 16 03:34:30.537: EPM_SESS_EVENT: **Executed [ip access-list extended**
xACSACLx-IP-MAB-FAIL-ACL-528741f3] command through parse_cmd. Result= 0

*Nov 16 03:34:30.538: EPM_SESS_EVENT: Executed [1 permit icmp any any]
command through parse_cmd. Result= 0

*Nov 16 03:34:30.539: EPM_SESS_EVENT: Executed [end] command through parse_cmd.
Result= 0

*Nov 16 03:34:30.541: EPM_SESS_EVENT: **ACL xACSACLx-IP-MAB-FAIL-ACL-528741f3**
provisioning successful

*Nov 16 03:34:31.136: EPM_SESS_EVENT: Successful feature attrs provided for
SM ACCOUNTING PLUG-IN

*Nov 16 03:34:31.136: EPM_SESS_EVENT: Successful feature attrs provided for
EPM ACL PLUG-IN

*Nov 16 03:34:31.136: AUTH-EVENT: Rcvd IPC call for pre 0x5F000002, inst
0xB2000072, hdl 0x95000073

*Nov 16 03:34:31.136: AUTH-EVENT: **Raising ext evt Template Activated (8)**
on session 0xCC000363, client (unknown) (0), hdl 0x00000000, attr_list

0xA5000E24

*Nov 16 03:34:31.142: AUTH-EVENT: [dc7b.94a3.7005, Gi1/0/1] Handling external
PRE event Template Activated for context 0xCC000363.

Когда нет никакого корректного профиля авторизации на ISE, он сообщает:

11001 Полученный Access-Request RADIUS
11017 RADIUS создал новый сеанс
11003 Возвращенный Access-Reject RADIUS

Кроме того, **сообщение об ошибках Аутентификации События 5400** представлено, но не показано больше подробных данных. После создания имени пользователя с паролем **cisco123** ошибка остается тем же, даже когда существует корректная Аутентификация/Правила авторизации. Единственное требование для имени той функции работает, правильно должен иметь корректный профиль авторизации.

Дополнительные сведения

- [Основанное на идентичности руководство по конфигурации сетевых сервисов, выпуск 3SE Cisco IOS XE](#)
- [Справочник по командам консолидированной платформы, Cisco IOS XE 3.2SE](#)
- [Cisco Systems – техническая поддержка и документация](#)