

# 目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[ローカルで定義されたサービス テンプレート](#)

[ISE で定義されるテンプレートを保守して下さい](#)

[ISE 設定](#)

[Catalyst 3850 シリーズ スイッチ設定](#)

[確認](#)

[ローカルで定義されたサービス テンプレート](#)

[ISE で定義されるテンプレートを保守して下さい](#)

[トラブルシューティング](#)

[ローカルで定義されたサービス テンプレート](#)

[ISE で定義されるテンプレートを保守して下さい](#)

[関連情報](#)

## 概要

この資料にセッションわかっているネットワーク フレームワークと Cisco Catalyst 3850 シリーズの識別 サービスを設定する方法を切り替えます記述されています。これは識別 サービス ( 802.1X、MAC 認証 バイパス ( MAB ) を設定する柔軟性および機能性を可能にする新しい方法 WebAuth ) です。それはローカルでまたは Cisco Identity Services Engine ( ISE ) サーバで保存することができるサービス テンプレートと共に Cisco 一般的な 分類 ポリシー言語 ( C3PL ) を使用します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Catalyst 3850 シリーズは、Cisco IOS<sup>®</sup> CLI 切り替えます
- Cisco ISE
- 識別 サービス ( 802.1x/MAB/WebAuth )

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Catalyst 3850 シリーズは、Cisco IOSバージョン 03.03.00SE またはそれ以降切り替えます
- Cisco ISE バージョン 1.2 以降

注 サポートマトリックスを表示するために [IBNS 2.0 配置ガイド](#)を参照して下さい。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

## 背景説明

サービス テンプレートは制御方策の特定の操作によってユーザセッションに接続することができる一組のポリシー属性が含まれています。2つの例はこの資料で示されます:

- MAB および障害シナリオに使用するローカルで定義されたサービス テンプレート。
- MAB および障害シナリオに使用する ISE 定義されたサービス テンプレート。

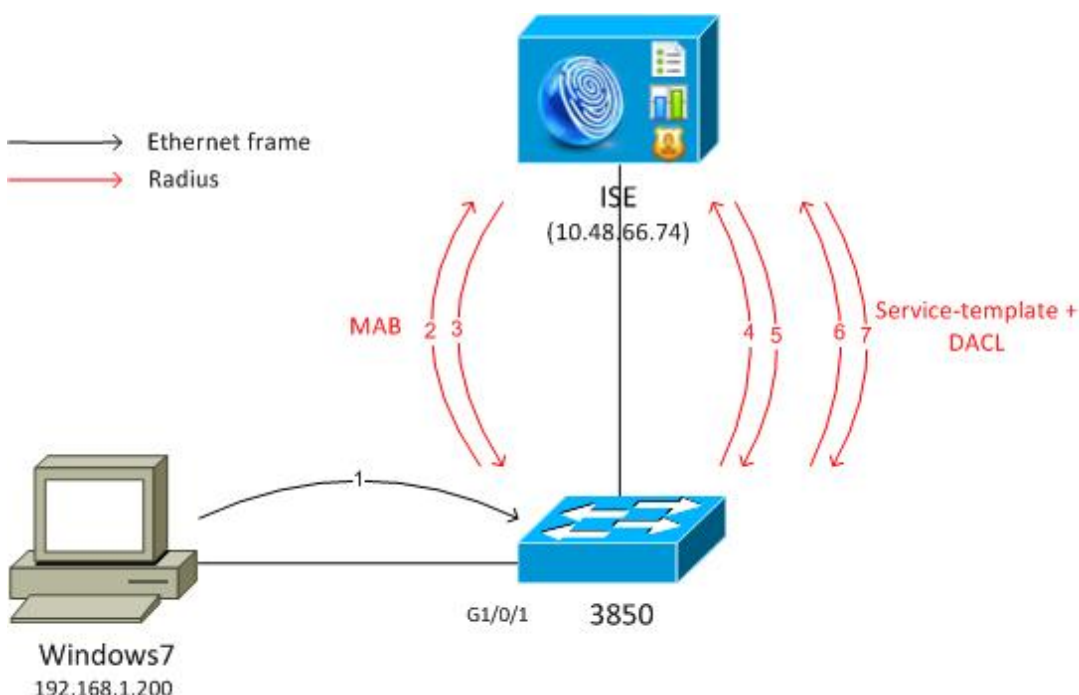
MAB はこの資料でように例使用されます。ただし、802.1X や WebAuth を使用し、C3PL と複雑なポリシーを構築することは可能性のあるです。

## 設定

注 このセクションで使用されているコマンドの詳細を調べるには、[Command Lookup Tool](#) ( [登録](#) ユーザ専用 ) を使用してください。

## ネットワーク図

ここに示される例は両方とも Windows PC を含みますスイッチに接続する MAB を行う。Windows MAC アドレスは MAB がなぜ失敗するかである ISE で設定されません。それから、スイッチはサービス テンプレートで定義されるポリシーを適用します。



## ローカルで定義されたサービス テンプレート

MAB 失敗の後で、スイッチはローカルで定義されたサービス テンプレートを加えます。

ここで、フローを示します。

1. Windows はイーサネットフレームを送信 します。
2. スイッチは MAB を行い、ユーザ名として MAC アドレスの ISE の方の RADIUS 要求を送信 します。
3. ISE はこと設定されるエンドポイントおよび戻り半径リジェクト持っていない。
4. スイッチはローカルで定義されたテンプレート ポリシー MAB\_FAIL をアクティブにします。

完全情報詳細については、[Identity Based Networking Service コンフィギュレーション ガイドを、Cisco IOS XE リリース 3SE \( Catalyst 3850 スイッチ \)](#) 参照して下さい。

基本的な例はここにあります:

```
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
```

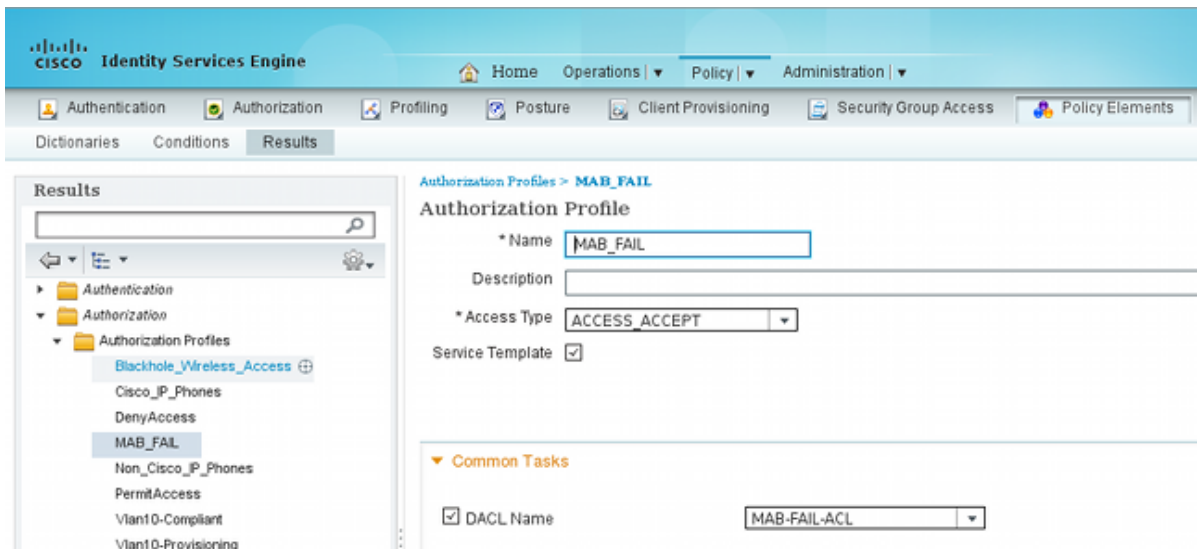
## ISE で定義されるテンプレートを保守して下さい

ここで、フローを示します。

1. Windows はイーサネットフレームを送信 します。
2. スイッチは MAB を行い、ユーザ名として MAC アドレスの ISE の方の RADIUS要求を送信 します。
3. ISE はこと設定されるエンドポイント持たないし半径リジェクトを戻します。
4. スイッチは ISE 認証、許可、アカウントिंग ( AAA ) のテンプレート ポリシー **MAB\_FAIL** を-リスト アクティブにします。 RADIUS要求はテンプレート名 ( **MAB\_FAIL** ) およびハードコードされたパスワードとしてユーザ名と送信 されます: **cisco123**. また、Cisco 属性値 ( AV ) ペアは接続された **download-request=service-template** です。
5. その AVペアはサービス テンプレート 要求としてその要求を扱うために ISE を強制します 。 すべて認証 および 権限ルールがあるように省略されます確認します。 ISE は同じネーム ( **MAB\_FAIL** ことを ) 存在でかどうかその時だけ許可 プロファイル チェックします。 ローカルユーザストアの **MAB\_FAIL** ユーザを設定する必要がありません。 それから、この例のダウンロード可能 アクセス制御リスト ( DACL ) である ISE はそのプロファイルと関連付けられるすべての属性を戻します。
6. DACL がスイッチでキャッシュされない場合、そのための別の RADIUS要求を DACL 送信 します。
7. DACL コンテンツは戻ります。 スイッチはポリシーを適用します。

## ISE 設定

ネットワーク アクセス デバイスを追加した後、許可 プロファイルが必要となります:



サービス テンプレート チェックボックスをチェックし、スイッチで定義されるものと同じ名前を使用することは重要です。

## Catalyst 3850 シリーズ スイッチ設定

この設定に最初の例からの 4 つの違いがあります:

- ローカル MAB\_FAIL\_LOCAL ポリシー テンプレートは取除かれます。
- 許可 ( CoA ) サポートの変更は追加されます。
- MAB\_FAIL ポリシー テンプレート ( ISE で設定されるポリシー ) のための ISE リストは使用されます。
- サービス テンプレート検索のための AAA 認証リストは指名されます。

次に設定を示します。

```

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
```

スイッチのテンプレートをアップデートするために CoA を送信 するので ISE のテンプレート ( 許可 プロファイル ) を変更した後スイッチの RADIUS CoA サポートを設定して下さい。

## 確認

### ローカルで定義されたサービス テンプレート

Catalyst 3850 シリーズでユーザセッションを確認するためにこのコマンドを切り替えて下さい、入力して下さい:

```
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
```

## ISE で定義されるテンプレートを保守して下さい

Catalyst 3850 シリーズでユーザセッションを確認するためにこのコマンドを切り替えて下さい、入力して下さい:

```
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
```

状態が失敗されるがこと、特定のテンプレートおよび関連 DACL が適用することに注目して下さい:

```
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
```

Access Control List ( ACL ) はインターフェイスの下で見えません:

```
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#
```

ASIC ( ハードウェアがことを ) 正しくプログラムされればかどうか確認することは可能性のあるです:

```
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 0x1ffffffa00 [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)
```

持っている各ユーザセッションは異なる DACL ために ASIC でプログラムされる別途のエントリがあります。ISE で、3 別々の認証があります:

- 壊れる MAB
- 正常なサービス テンプレート 検索 ( MAB\_FAIL )
- 正常な DACL 検索

		#ACSACL#-IP-MAB-FAIL-ACL-528741f3	
		MAB_FAIL	
		DC:7B:94:A3:70:05	DC:7B:94:A3:70:05

サービス テンプレートのための要求を受け取るときステップの詳細情報はここにあります:

- 11001 受け取った RADIUS Access-Request
- 11017 RADIUS は新しいセッションを作成しました
- 11022 許可 プロファイルで規定された dACL を追加しました
- 11002 戻された RADIUS Access-Accept

これは認証/許可ルールが処理されないことを明らかに示します。

## トラブルシューティング

### ローカルで定義されたサービス テンプレート

現在のシナリオのためのデバッグはここにあります。いくつかの出力は明確にするために省略されます:

```
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, Gi1/0/1] **New client dc7b.94a3.7005** - client handle 0x00000001 for SVM

\*Nov 16 11:45:11.347: AUTH-DETAIL: [dc7b.94a3.7005, Gi1/0/1] Create attr list, session 0x50000368:

\*Nov 16 11:45:11.347: AUTH-DETAIL: [dc7b.94a3.7005, Gi1/0/1] - adding MAC dc7b.94a3.7005

\*Nov 16 11:45:11.347: AUTH-DETAIL: [dc7b.94a3.7005, Gi1/0/1] - adding Swidb 0x38A8DABC

\*Nov 16 11:45:11.348: AUTH-DETAIL: [dc7b.94a3.7005, Gi1/0/1] - adding AAA\_ID=117D

\*Nov 16 11:45:11.348: AUTH-DETAIL: [dc7b.94a3.7005, Gi1/0/1] - adding Audit\_sid=0A30276F0000117D52D8816C

\*Nov 16 11:45:11.348: AUTH-DETAIL: [dc7b.94a3.7005, Gi1/0/1] - adding IIF ID=0x1091E8000000B0

\*Nov 16 11:45:11.348: AUTH-EVENT: [dc7b.94a3.7005, Gi1/0/1] **Policy processing started** for 0x50000368(dc7b.94a3.7005)

\*Nov 16 11:45:11.348: AUTH-EVENT: [dc7b.94a3.7005, Gi1/0/1] 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]

```

## ISE で定義されるテンプレートを保守して下さい

現在のシナリオのためのデバッグはここにあります。いくつかの出力は明確にするために省略されます:

<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.

```

ISE に正しい許可プロファイルがないとき、報告します:

- 11001 受け取った RADIUS Access-Request
- 11017 RADIUS は新しいセッションを作成しました
- 11003 戻された RADIUS Access-Reject

また、イベント 5400 認証 失敗通知メッセージは示されますが、これ以上の詳細は明らかにされません。cisco123 パスワードでユーザ名を作成した後、エラーは正しい認証/許可ルールがある時でさえ、変わりません。機能作業が正しく正しい許可プロファイルを持つことであること持つべき唯一の要件。

## 関連情報

- [Identity Based Networking Service コンフィギュレーションガイド、Cisco IOS XE リリース](#)

### 3SE

- [強化されたプラットフォーム コマンドレファレンス、Cisco IOS XE 3.2SE](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)