

# Informazioni sulle implementazioni di EAP-FAST e Chaining su AnyConnect NAM e ISE

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Teoria](#)

[Fasi](#)

[PAC](#)

[Quando vengono generate le PAC](#)

[EAP-FAST Server Master Key ACS 4.x rispetto ad ACS 5x e ISE](#)

[Ripresa della sessione](#)

[Stato server](#)

[Senza stato \(basato su PAC\)](#)

[Implementazione di AnyConnect NAM](#)

[Preparazione PAC \(fase 0\)](#)

[Tunnel TLS anonimo](#)

[Tunnel TLS autenticato](#)

[Concatenamento EAP](#)

[Dove sono memorizzati i file PAC](#)

[AnyConnect NAM 3.1 e 4.0](#)

[Esempi](#)

[Esempio di rete](#)

[EAP-Fast senza concatenamento EAP con PAC utente e macchina](#)

[EAP-Fast con concatenamento EAP con riconnessione rapida PAC](#)

[EAP-Fast con concatenamento EAP senza PAC](#)

[EAP-Fast con scadenza PAC autorizzazione concatenamento EAP](#)

[EAP-Fast con PAC tunnel di concatenamento EAP scaduto](#)

[EAP-Fast con concatenamento EAP e provisioning PAC tunnel TLS anonimo](#)

[EAP-Fast con solo autenticazione utente concatenamento EAP](#)

[EAP-Fast con concatenamento EAP e impostazioni del tunnel TLS anonimo incoerenti](#)

[Risoluzione dei problemi](#)

[ISE](#)

[AnyConnect NAM](#)

[Riferimenti](#)

## Introduzione

Questo articolo spiega i dettagli relativi alle implementazioni EAP-FAST su Cisco AnyConnect Network Access Manager (NAM) e Identity Services Engine (ISE). Viene inoltre illustrato il funzionamento congiunto di caratteristiche specifiche e vengono forniti esempi e casi di utilizzo tipici.

# Prerequisiti

## Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base del framework EAP e dei metodi EAP-FAST
- Conoscenze base di Identity Services Engine (ISE)
- Conoscenze base di AnyConnect NAM e dell'Editor di profili
- Conoscenze base della configurazione di Cisco Catalyst per i servizi 802.1x

## Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

- Windows 7 con Cisco AnyConnect Secure Mobility Client, versione 3.1 e 4.0
- Switch Cisco Catalyst 3750X con software 15.2.1 e versioni successive
- Cisco ISE, release 1.4

# Teoria

## Fasi

EAP-FAST è un metodo EAP flessibile che consente l'autenticazione reciproca di un richiedente e di un server. È simile a EAP-PEAP, ma in genere non richiede l'utilizzo di certificati client o server. Uno dei vantaggi di EAP-FAST è la capacità di concatenare più autenticazioni (utilizzando più metodi interni) e di associarle tramite crittografia (concatenamento EAP). Le implementazioni Cisco utilizzano questa funzionalità per l'autenticazione di computer e utenti.

EAP-FAST utilizza le credenziali di accesso protetto (PAC) per stabilire rapidamente il tunnel TLS (ripresa della sessione) o per autorizzare l'utente/computer (ignora il metodo interno per l'autenticazione).

Per EAP-FAST sono previste 3 fasi:

- fase 0 (preparazione PAC)
- fase 1 (creazione del tunnel TLS)
- fase 2 (autenticazione)

EAP-FAST supporta le conversazioni senza PAC e basate su PAC. La PAC-based consiste nella preparazione della PAC e nell'autenticazione basata sulla PAC. La preparazione della PAC può essere basata su una sessione TLS anonima o autenticata.

## PAC

La PAC è costituita dalle credenziali di accesso protetto generate dal server e fornite al client. Esso comprende:

- Chiave PAC (valore segreto casuale, utilizzato per derivare le chiavi master e di sessione)

TLS)

- PAC opaco (chiave PAC + identità utente - tutto crittografato con chiave master del server EAP-FAST)
- Informazioni PAC (identità server, timer TTL)

Il server che emette la PAC cripta la chiave e l'identità della PAC utilizzando la chiave master del server EAP-FAST (opaca per la PAC) e invia l'intera PAC al client. Non conserva/memorizza altre informazioni (ad eccezione della chiave master che è la stessa per tutte le PAC).

Una volta ricevuta, l'opacità della PAC viene decriptata utilizzando la chiave master del server EAP-FAST e convalidata. La chiave PAC viene utilizzata per derivare il master TLS e le chiavi di sessione per un tunnel TLS abbreviato.

Le nuove chiavi master del server EAP-FAST vengono generate alla scadenza della chiave master precedente. In alcuni casi è possibile revocare una chiave master.

Attualmente si utilizzano alcuni tipi di PAC:

- PAC tunnel: utilizzata per la definizione del tunnel TLS (senza la necessità di un certificato client o server). Hello inviato nel client TLS
- PAC computer: utilizzato per la creazione del tunnel TLS e l'autorizzazione immediata della macchina. Hello inviato nel client TLS
- PAC autorizzazione utente: utilizzato per l'autenticazione utente immediata (ignora metodo interno) se consentito dal server. Inviato all'interno del tunnel TLS utilizzando TLV.
- PAC autorizzazione computer: utilizzato per l'autenticazione immediata del computer (ignora metodo interno) se consentito dal server. Inviato all'interno del tunnel TLS utilizzando TLV.
- PAC Trustsec: utilizzato per l'autorizzazione durante l'aggiornamento dell'ambiente o dei criteri.

Tutte queste PAC vengono di solito consegnate automaticamente nella fase 0. Alcune PAC (tunnel, computer, trustsec) possono anche essere consegnate manualmente.

### Quando vengono generate le PAC

- PAC tunnel: eseguito dopo un'autenticazione riuscita (metodo interno) se non utilizzato in precedenza.
- Autorizzazione PAC: eseguito dopo l'autenticazione (metodo interno) se non utilizzato in precedenza.
- PAC computer: eseguito dopo l'autenticazione corretta del computer (metodo interno) se non viene utilizzato in precedenza e se non viene utilizzata una PAC di autorizzazione. Verrà fornito alla scadenza della PAC del tunnel, ma non alla scadenza della PAC di autorizzazione. Verrà eseguito il provisioning quando EAP-Chaining è abilitato o disabilitato.

Nota:

Ogni preparazione PAC richiede l'autenticazione corretta, ad eccezione dei seguenti casi di utilizzo: Un utente autorizzato richiede la PAC del computer per un computer che non dispone di un account AD.

La tabella seguente riepiloga le funzionalità di provisioning e di aggiornamento proattivo:

Tipo PAC	Tunnel v1/v1a/CTS	Macchina	Authorization
Fornire PAC su richiesta	sì	solo su provisioning	solo su provisioning

per l'approvvigionamento		autenticato	autenticato e se è richiesto anche la PAC del tunnel solo se non è stato utilizzato in questa autenticazione
Fornisci PAC su richiesta all'autenticazione	sì	sì	no
Aggiornamento proattivo Quando si esegue il fallback alla preparazione della PAC dopo un errore di autenticazione basata sulla PAC (ad esempio quando la PAC è scaduta)	sì	no	no
Supporto ACS 4.x PAC	rifiuta e non fornisci la nuova	rifiuta e non fornisci la nuova	rifiuta e non fornisci la nuova
	per la PAC tunnel v1/v1a	sì	no

## EAP-FAST Server Master Key ACS 4.x rispetto ad ACS 5x e ISE

C'è una leggera differenza nella gestione della chiave master quando si confrontano ACS 4.x e ISE

Funzionalità ACS 4.1.2	ACS 5.x/ISE
Chiave master La chiave master ha TTL, può essere attiva, ritirata o scaduta	La chiave master viene generata automaticamente dal valore di inizializzazione in ogni periodo di tempo configurato. Chiave master specifica sempre accessibile e mai scaduta
Aggiornamento PAC L'aggiornamento della PAC viene inviato dal server quando la PAC è scaduta, a meno che la chiave master utilizzata per la crittografia della PAC non sia scaduta	L'aggiornamento delle PAC viene inviato dal server dopo la prima autenticazione riuscita eseguita in un periodo di tempo configurabile specifico prima del momento di scadenza delle PAC.

In altre parole, ISE conserverà tutte le vecchie chiavi master e ne genererà una nuova per impostazione predefinita una volta alla settimana. Poiché la chiave master non può scadere, verrà convalidata solo la TTL PAC.

Il periodo di generazione della chiave master ISE è configurato da *Amministrazione -> Impostazioni -> Protocollo -> EAP-FAST -> Impostazioni EAP-FAST*.

## Ripresa della sessione

Questo è un componente importante che consente l'uso della PAC del tunnel. Consente la rinegoziazione del tunnel TLS senza l'utilizzo di certificati.

Per EAP-FAST sono disponibili due tipi di curriculum: Basato sullo stato del server e senza stato (basato su PAC).

## Stato server

Il metodo basato su TLS standard è basato sul SessionID TLS memorizzato nella cache del server. Il client che invia il messaggio Hello del client TLS collega l'ID sessione per riprendere la sessione. La sessione viene utilizzata solo per la preparazione PAC quando si utilizza un tunnel TLS anonimo:

Source	Destination	Protocol	Length	Info	User-Name
10.62.148.109	10.48.17.14	RADIUS	378	Access-Request(1) (id=9, l= anonymous	
10.48.17.14	10.62.148.109	RADIUS	86	Access-Reject(3) (id=9, l=4	
10.62.148.109	10.48.17.14	RADIUS	301	Access-Request(1) (id=30, l anonymous	
10.48.17.14	10.62.148.109	RADIUS	193	Access-Challenge(11) (id=30	
10.62.148.109	10.48.17.14	RADIUS	510	Access-Request(1) (id=31, l anonymous	

Length: 138

Type: Flexible Authentication via Secure Tunneling EAP (EAP-FAST) (43)

▷ EAP-TLS Flags: 0x01

▽ Secure Sockets Layer

▽ TLSv1 Record Layer: Handshake Protocol: Client Hello

Content Type: Handshake (22)

Version: TLS 1.0 (0x0301)

Length: 127

▽ Handshake Protocol: Client Hello

Handshake Type: Client Hello (1)

Length: 123

Version: TLS 1.0 (0x0301)

▷ Random

Session ID Length: 32

Session ID: 9a344ae351082ec6dbaafb8509cf99b4fa664574b6272f876...

Cipher Suites Length: 52

▷ Cipher Suites (26 suites)

Compression Methods Length: 1

▷ Compression Methods (1 method)

## Senza stato (basato su PAC)

La PAC Autorizzazione utente/computer viene utilizzata per archiviare gli stati di autenticazione e autorizzazione precedenti per il peer.

Il ripristino sul lato client è basato sulla RFC 4507. Il server non deve memorizzare dati nella cache; il client collega invece la PAC nell'estensione Hello SessionTicket del client TLS. A sua volta, la PAC viene convalidata dal server. Esempio basato sulla PAC del tunnel consegnata al server:

	Source	Destination	Protocol	Length	Info	User-Name
23	10.62.148.109	10.48.17.14	RADIUS	301	Access-Request(1) (id=91, l=259)	anonymous
24	10.48.17.14	10.62.148.109	RADIUS	193	Access-Challenge(11) (id=91, l=151)	
25	10.62.148.109	10.48.17.14	RADIUS	666	Access-Request(1) (id=92, l=624)	anonymous
26	10.48.17.14	10.62.148.109	RADIUS	311	Access-Challenge(11) (id=92, l=269)	
27	10.62.148.109	10.48.17.14	RADIUS	437	Access-Request(1) (id=93, l=395)	anonymous
28	10.48.17.14	10.62.148.109	RADIUS	226	Access-Challenge(11) (id=93, l=184)	
29	10.62.148.109	10.48.17.14	RADIUS	468	Access-Request(1) (id=94, l=426)	anonymous
30	10.48.17.14	10.62.148.109	RADIUS	258	Access-Challenge(11) (id=94, l=216)	
31	10.62.148.109	10.48.17.14	RADIUS	516	Access-Request(1) (id=95, l=474)	anonymous
32	10.48.17.14	10.62.148.109	RADIUS	258	Access-Challenge(11) (id=95, l=216)	
33	10.62.148.109	10.48.17.14	RADIUS	452	Access-Request(1) (id=96, l=410)	anonymous

#### Secure Sockets Layer

##### ▼ TLSv1 Record Layer: Handshake Protocol: Client Hello

Content Type: Handshake (22)

Version: TLS 1.0 (0x0301)

Length: 281

##### ▼ Handshake Protocol: Client Hello

Handshake Type: Client Hello (1)

Length: 277

Version: TLS 1.0 (0x0301)

##### ▷ Random

Session ID Length: 0

Cipher Suites Length: 52

##### ▷ Cipher Suites (26 suites)

Compression Methods Length: 1

##### ▷ Compression Methods (1 method)

Extensions Length: 184

##### ▼ Extension: SessionTicket TLS

Type: SessionTicket TLS (0x0023)

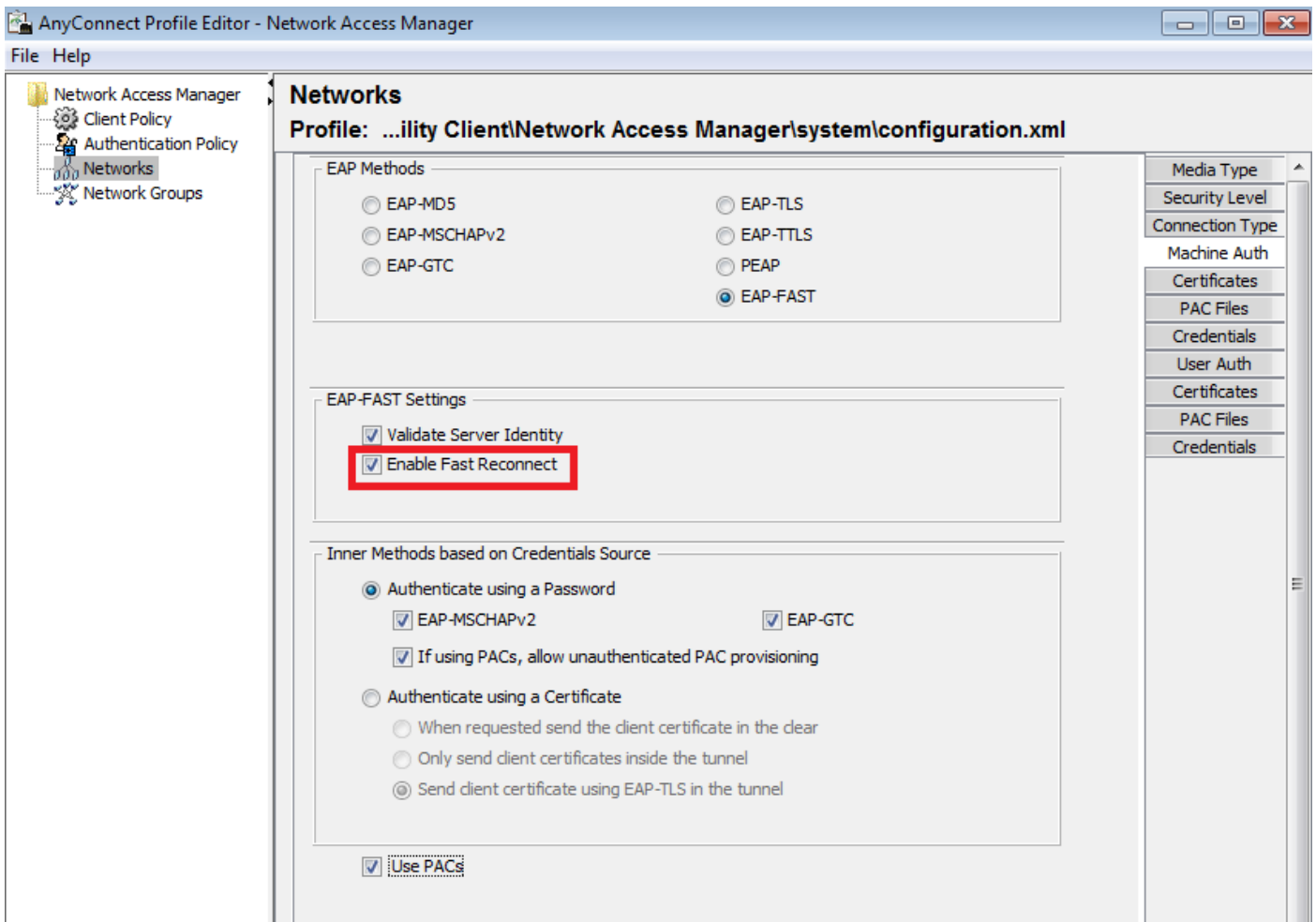
Length: 180

Data (180 bytes)

▷ AVP: l=18 t=Message-Authenticator(80): 0cb2477c076ea96d3ba150245e6291e8

## Implementazione di AnyConnect NAM

È abilitato sul lato client (AnyConnect NAM) tramite Fast Reconnect, ma viene usato solo per controllare l'utilizzo della PAC di autorizzazione.



Se l'impostazione è disabilitata, NAM continuerà a utilizzare la PAC del tunnel per creare il tunnel TLS (non sono necessari certificati). Tuttavia, non utilizzerà le PAC di autorizzazione per eseguire l'autorizzazione immediata dell'utente e del computer. Di conseguenza, la fase 2 con il metodo interno sarà sempre necessaria.

ISE ha un'opzione per abilitare la ripresa delle sessioni senza stato. E come in NAM è solo per Authorization PAC. L'uso della PAC del tunnel è controllato con le opzioni "Usa PAC".

Allow EAP-FAST

EAP-FAST Inner Methods

Allow EAP-MS-CHAPv2

Allow Password Change Retries  (Valid Range 0 to 3)

Allow EAP-GTC

Allow Password Change Retries  (Valid Range 0 to 3)

Allow EAP-TLS

Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy (i)

Use PACs  Don't Use PACs

Tunnel PAC Time To Live

Proactive PAC update will occur after  % of PAC Time To Live has expired

Allow Anonymous In-Band PAC Provisioning

Allow Authenticated In-Band PAC Provisioning

Server Returns Access Accept After Authenticated Provisioning

Accept Client Certificate For Provisioning

Allow Machine Authentication

Machine PAC Time To Live

Enable Stateless Session Resume

Authorization PAC Time To Live   (i)

Enable EAP Chaining

Preferred EAP Protocol

NAM tenterà di utilizzare le PAC se l'opzione è abilitata. Se la funzione "Don't Use PACs" è configurata in ISE e ISE riceve una PAC tunnel nell'estensione TLS, verrà segnalato il seguente errore e verrà restituito un errore EAP:

inserire qui

Nell'ISE, è anche necessario abilitare la ripresa della sessione in base all'ID sessione TLS (dalle impostazioni globali EAP-FAST). È disabilitata per impostazione predefinita:

### EAP FAST Settings

\* Authority Identity Info Description

\* Master Key Generation Period

Revoke all master keys and PACs

### PAC-less Session Resume

Enable PAC-less Session Resume

\* PAC-less Session Timeout



Tenere presente che è possibile utilizzare un solo tipo di curriculum di sessione. SessionID based viene utilizzato solo per le distribuzioni senza PAC, mentre RFC 4507 based viene utilizzato solo per le distribuzioni PAC.

## Preparazione PAC (fase 0)

Le PAC possono essere fornite automaticamente in fase 0. La fase 0 è costituita da:

- Creazione tunnel TLS
- Autenticazione (metodo interno)

Le PAC vengono recapitate dopo un'autenticazione riuscita all'interno del tunnel TLS tramite PAC TLV (e conferma PAC TLV)

## Tunnel TLS anonimo

Per le distribuzioni senza un'infrastruttura PKI, è possibile utilizzare un tunnel TLS anonimo. Il tunnel TLS anonimo verrà creato utilizzando la suite di cifratura Diffie Hellman, senza la necessità di un certificato server o client. Questo approccio è incline agli attacchi di Man in the Middle (rappresentazione).

Per utilizzare questa opzione, NAM richiede la seguente opzione configurata:

"Se si utilizzano le PAC, consentire la preparazione non autenticata delle PAC" (ciò è utile solo per il metodo interno basato su password, poiché senza l'infrastruttura PKI non è possibile utilizzare il metodo interno basato su certificato).

Inoltre, per ISE sarà necessario configurare quanto segue in base ai protocolli di autenticazione consentiti:

"Consenti preparazione PAC in banda anonima"

La preparazione anonima della PAC in banda viene utilizzata nelle distribuzioni NDAC TrustSec (sessione EAP-FAST negoziata tra dispositivi di rete).

## Tunnel TLS autenticato

Si tratta dell'opzione più sicura e consigliata. Il tunnel TLS viene generato in base al certificato del server convalidato dal supplicant. Ciò richiede un'infrastruttura PKI solo sul lato server, necessaria per ISE (su NAM è possibile disabilitare l'opzione "Convalida identità server").

Per ISE ci sono due opzioni aggiuntive:

- Allow Anonymous In-Band PAC Provisioning
- Allow Authenticated In-Band PAC Provisioning
  - Server Returns Access Accept After Authenticated Provisioning
  - Accept Client Certificate For Provisioning

Normalmente, dopo la preparazione della PAC, è necessario inviare un messaggio di rifiuto dell'accesso che impone al richiedente di riautenticarsi utilizzando le PAC. Tuttavia, poiché le PAC sono state consegnate nel tunnel TLS con autenticazione, è possibile abbreviare l'intero processo

e restituire l'autorizzazione di accesso subito dopo la preparazione delle PAC.

La seconda opzione consente di creare il tunnel TLS in base al certificato client (è necessaria la distribuzione di Infrastruttura a chiave pubblica sugli endpoint). In questo modo è possibile creare il tunnel TLS con l'autenticazione reciproca, che ignora il metodo interno e passa direttamente alla fase di preparazione della PAC. È importante fare attenzione in questo caso: a volte il richiedente presenterà un certificato non considerato attendibile da ISE (destinato ad altri scopi) e la sessione avrà esito negativo.

## Concatenamento EAP

Consente l'autenticazione di utenti e computer in una sessione Radius/EAP. È possibile concatenare più metodi EAP. Al termine della prima autenticazione (in genere il computer), il server invierà un TLV a risultato intermedio (all'interno del tunnel TLS) per indicare che l'operazione è riuscita. Tale TLV deve essere accompagnato da una richiesta TLV di cryptobinding. L'associazione tramite crittografia viene utilizzata per dimostrare che sia il server che il peer hanno partecipato alla sequenza specifica di autenticazioni. Il processo di cryptobinding utilizza il materiale per le chiavi della fase 1 e della fase 2. Viene inoltre allegato un altro TLV: EAP-Payload - Avvio della nuova sessione (in genere per l'utente). Una volta che il server radius (ISE) riceve la risposta TLV di crypto-binding e la convalida, nel log verranno visualizzati i dati seguenti e verrà tentato il metodo EAP successivo (in genere per l'autenticazione dell'utente):

```
12126 EAP-FAST cryptobinding verification passed
```

Se la convalida di cryptobinding ha esito negativo, l'intera sessione EAP avrà esito negativo. Se una delle autenticazioni in ha avuto esito negativo, l'operazione è comunque corretta. Di conseguenza, ISE consente a un amministratore di configurare più risultati di concatenamento in base alla condizione di autorizzazione NetworkAccess:EapChainingResult:

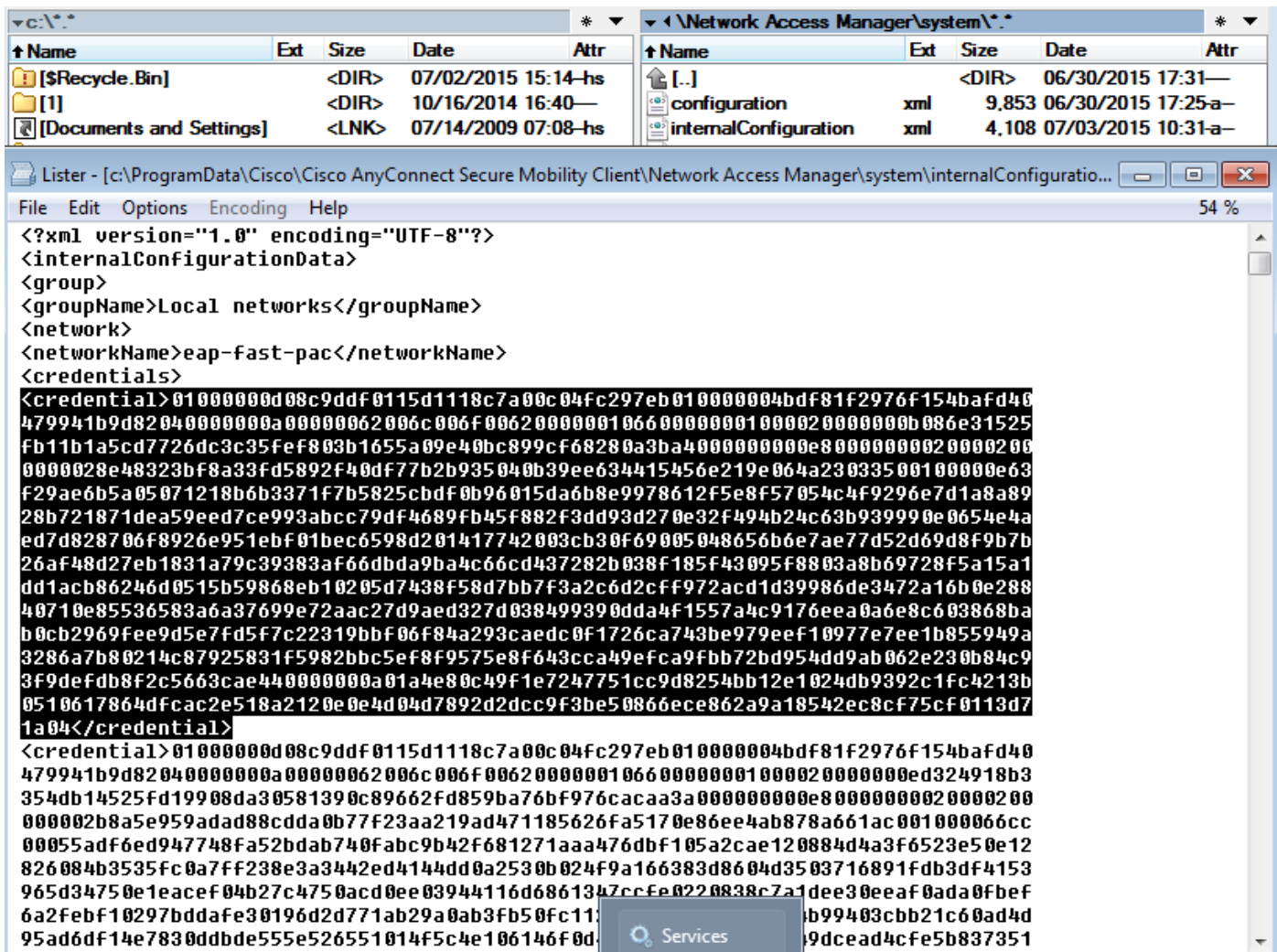
- No chaining
- User and machine both succeeded
- User failed and machine succeeded
- User succeeded and machine failed

Il concatenamento EAP viene attivato automaticamente in NAM quando l'autenticazione utente e computer EAP-FAST è attivata.

Il concatenamento EAP deve essere configurato in ISE.

## Dove sono memorizzati i file PAC

Per impostazione predefinita, le PAC tunnel e computer sono memorizzate in C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\system\internalConfiguration.xml nelle sezioni <credenziale>. Questi file vengono archiviati in forma crittografata.

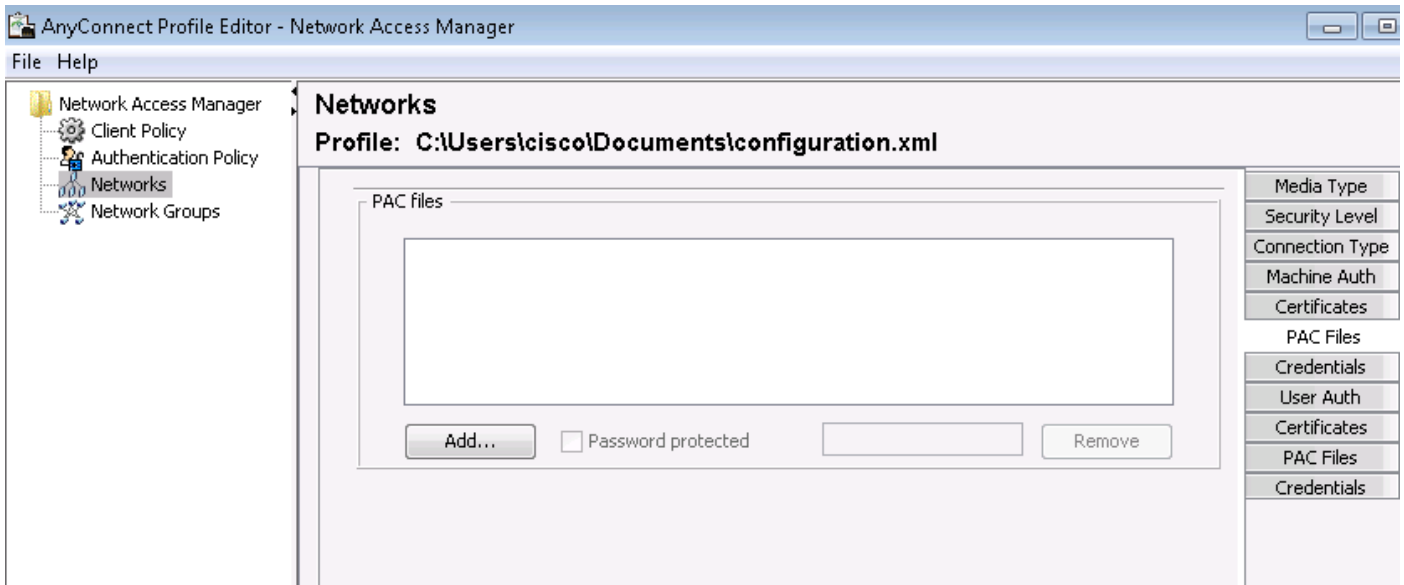


Le PAC di autorizzazione vengono memorizzate solo in memoria e vengono rimosse dopo il riavvio o il riavvio del servizio NAM.

È necessario riavviare il servizio per rimuovere la PAC del tunnel o del computer.

## AnyConnect NAM 3.1 e 4.0

L'editor di profili AnyConnect 3.x NAM ha consentito all'amministratore di configurare manualmente le PAC. Questa funzionalità è stata rimossa dall'editor dei profili AnyConnect 4.x NAM.

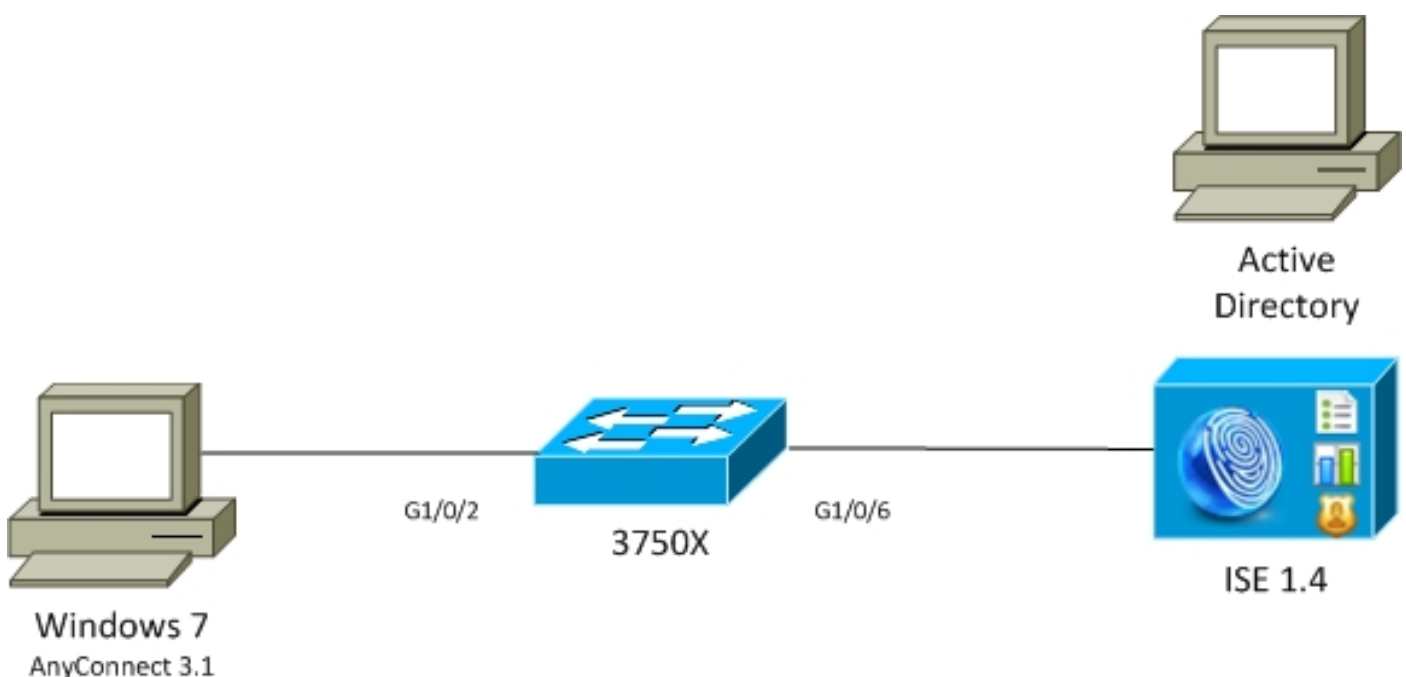


La decisione di rimuovere tale funzionalità si basa su [CSCuf31422](#) e [CSCua13140](#).

## Esempi

### Esempio di rete

Tutti gli esempi sono stati testati utilizzando la seguente topologia di rete. Lo stesso vale per l'uso di wireless.



### EAP-Fast senza concatenamento EAP con PAC utente e macchina

Per impostazione predefinita, EAP\_chaining è disabilitato in ISE. Tuttavia, tutte le altre opzioni sono abilitate, comprese le PAC di autorizzazione e macchina. Il supplicante dispone già di una credenziale di accesso protetta per computer e tunnel valida. In questo flusso, ci saranno due autenticazioni separate - una per il computer e una per l'utente - con log separati su ISE. Le fasi principali sono state registrate da ISE. Prima autenticazione (computer):

- Il richiedente invia al client TLS Hello con PAC computer.
- Il server convalida la PAC del computer e crea il tunnel TLS (non vengono utilizzati certificati).
- Il server convalida la PAC del computer ed esegue la ricerca dell'account in Active Directory e ignora il metodo interno.

12102 Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as negotiated

**12800 Extracted first TLS record; TLS handshake started**

**12174 Received Machine PAC**

12805 Extracted TLS ClientHello message

12806 Prepared TLS ServerHello message

12801 Prepared TLS ChangeCipherSpec message

**12816 TLS handshake succeeded**

**12132 EAP-FAST built PAC-based tunnel for purpose of authentication**

**24351 Account validation succeeded**

**24420 User's Attributes retrieval from Active Directory succeeded - example.com**

**22037 Authentication Passed**

**12124 EAP-FAST inner method skipped**

11503 Prepared EAP-Success

11002 Returned RADIUS Access-Accept

Seconda autenticazione (utente):

- Il richiedente invia al client TLS il messaggio Hello con la PAC del tunnel.
- Il server convalida la PAC e crea il tunnel TLS (non vengono utilizzati certificati).
- Poiché il richiedente non dispone di una PAC di autorizzazione, per l'autenticazione viene utilizzato il metodo interno (EAP-MSCHAP).

12102 Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as negotiated

**12800 Extracted first TLS record; TLS handshake started**

**12175 Received Tunnel PAC**

12805 Extracted TLS ClientHello message

12806 Prepared TLS ServerHello message

12801 Prepared TLS ChangeCipherSpec message

**12816 TLS handshake succeeded**

**12132 EAP-FAST built PAC-based tunnel for purpose of authentication**

**12125 EAP-FAST inner method started**

11806 Prepared EAP-Request for inner method proposing **EAP-MSCHAP** with challenge

**24402 User authentication against Active Directory succeeded - example.com**

**22037 Authentication Passed**

11503 Prepared EAP-Success

11002 Returned RADIUS Access-Accept

Nella sezione "Altri attributi" del report dettagliato in ISE, si nota quanto segue per l'autenticazione sia dell'utente che del computer:

EapChainingResult: **No chaining**

## EAP-Fast con concatenamento EAP con riconnessione rapida PAC

In questo flusso, il supplicant dispone già di una PAC tunnel valida insieme alle PAC di

autorizzazione utente e macchina:

- Il richiedente invia al client TLS il messaggio Hello con la PAC del tunnel.
- Il server convalida la PAC e crea il tunnel TLS (non vengono utilizzati certificati).
- ISE avvia il concatenamento EAP. Il richiedente allega le PAC di autorizzazione per utente e computer utilizzando il TLV all'interno del tunnel TLS.
- ISE convalida le PAC di autorizzazione (non è necessario alcun metodo interno), verifica che gli account siano presenti in Active Directory (nessuna autenticazione aggiuntiva), ha esito positivo.

```
12102  Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as negotiated
12800  Extracted first TLS record; TLS handshake started
12175  Received Tunnel PAC
12805  Extracted TLS ClientHello message
12806  Prepared TLS ServerHello message
12801  Prepared TLS ChangeCipherSpec message

12816  TLS handshake succeeded
12132  EAP-FAST built PAC-based tunnel for purpose of authentication
12209  Starting EAP chaining
12210  Received User Authorization PAC
12211  Received Machine Authorization PAC

24420  User's Attributes retrieval from Active Directory succeeded - example.com
22037  Authentication Passed

24439  Machine Attributes retrieval from Active Directory succeeded - example.com
22037  Authentication Passed

11503  Prepared EAP-Success
11002  Returned RADIUS Access-Accept
```

Nella sezione "Altri attributi" del report dettagliato in ISE, si nota quanto segue:

EapChainingResult: **EAP Chaining**

Inoltre, le credenziali utente e computer sono incluse nello stesso registro come illustrato di seguito:

Username: cisco,host/mgarcarz-PC

## EAP-Fast con concatenamento EAP senza PAC

In questo flusso, NAM è configurato per non utilizzare una PAC, ISE è configurato anche per non utilizzare la PAC (ma con il concatenamento EAP)

- Il supplicant invia al client TLS Hello senza la PAC del tunnel.
- Il server risponde con i payload del certificato TLS e della richiesta di certificato.
- Il supplicant deve considerare attendibile il certificato del server, non invierà alcun certificato client (payload del certificato uguale a zero). È stato generato il tunnel TLS.
- L'ISE invia una richiesta TLV per il certificato del client all'interno del tunnel TLS, ma il richiedente no (non è necessario averlo per continuare).
- Avvia Concatenamento EAP per l'utente, utilizzando il metodo interno con l'autenticazione MSCHAPv2.

- Continua con l'autenticazione del computer, utilizzando il metodo interno con l'autenticazione MSCHAPv2.
- Non è stato eseguito il provisioning delle PAC.

```

12102      Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST
as negotiated
12800      Extracted first TLS record; TLS handshake started
12805      Extracted TLS ClientHello message
12806      Prepared TLS ServerHello message
12807      Prepared TLS Certificate message
12809      Prepared TLS CertificateRequest message
12811      Extracted TLS Certificate message containing client certificate
12812      Extracted TLS ClientKeyExchange message

12816      TLS handshake succeeded
12207      Client certificate was requested but not received during tunnel establishment. Will
renegotiate and request client certificate inside the tunnel.
12226      Started renegotiated TLS handshake

12104      Extracted EAP-Response containing EAP-FAST challenge-response
12811      Extracted TLS Certificate message containing client certificate
12812      Extracted TLS ClientKeyExchange message
12804      Extracted TLS Finished message
12801      Prepared TLS ChangeCipherSpec message
12802      Prepared TLS Finished message
12226      Started renegotiated TLS handshake
12205      Client certificate was requested but not received inside the tunnel. Will continue
with inner method.
12176      EAP-FAST PAC-less full handshake finished successfully

12209      Starting EAP chaining
12218      Selected identity type 'User'

11806      Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge

24402      User authentication against Active Directory succeeded - example.com
22037      Authentication Passed

12219      Selected identity type 'Machine'

11806      Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge

24470      Machine authentication against Active Directory is successful - example.com
22037      Authentication Passed

11503      Prepared EAP-Success
11002      Returned RADIUS Access-Accept

```

## EAP-Fast con scadenza PAC autorizzazione concatenamento EAP

In questo flusso, il richiedente dispone di una PAC tunnel valida ma ha una PAC di autorizzazione scaduta:

- Il richiedente invia al client TLS il messaggio Hello con la PAC del tunnel.
- Il server convalida la PAC e crea il tunnel TLS (non vengono utilizzati certificati).
- ISE avvia il concatenamento EAP. Il richiedente allega le PAC di autorizzazione per utente e macchina utilizzando TLV all'interno del tunnel TLS.
- Quando le PAC sono scadute, viene avviato il metodo interno per l'utente e per il computer (EAP-MSCHAP).

- Una volta completate entrambe le autenticazioni, vengono fornite le PAC di autorizzazione utente e computer.

```

12102  Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as
negotiated
12800  Extracted first TLS record; TLS handshake started
12175  Received Tunnel PAC
12805  Extracted TLS ClientHello message
12806  Prepared TLS ServerHello message
12801  Prepared TLS ChangeCipherSpec message

12816  TLS handshake succeeded
12132  EAP-FAST built PAC-based tunnel for purpose of authentication
12209  Starting EAP chaining
12227  User Authorization PAC has expired - will run inner method
12228  Machine Authorization PAC has expired - will run inner method
12218  Selected identity type 'User'

11806  Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge

24402  User authentication against Active Directory succeeded - example.com
22037  Authentication Passed

12219  Selected identity type 'Machine'

24470  Machine authentication against Active Directory is successful - example.com
22037  Authentication Passed

12171  Successfully finished EAP-FAST user authorization PAC provisioning/update
12179  Successfully finished EAP-FAST machine authorization PAC provisioning/update

11503  Prepared EAP-Success
11002  Returned RADIUS Access-Accept

```

## EAP-Fast con PAC tunnel di concatenamento EAP scaduto

In questo flusso quando non esiste una PAC del tunnel valida, si verifica una negoziazione TLS completa con fase interna.

- Il richiedente invia al client TLS il messaggio Hello senza la PAC del tunnel.
- Il server risponde con i payload del certificato TLS e della richiesta di certificato.
- Il supplicant deve considerare attendibile il certificato del server, non invierà il certificato client (payload del certificato uguale a zero), tunnel TLS generato.
- ISE invia una richiesta TLV per il certificato client all'interno del tunnel TLS, ma il richiedente non la riceve (non è necessario averla per continuare).
- Avvia Concatenamento EAP per l'utente, utilizzando il metodo interno con l'autenticazione MSCHAPv2.
- Continua con l'autenticazione del computer, utilizzando il metodo interno con l'autenticazione MSCHAPv2.
- Provisioning di tutte le PAC completato (abilitato nella configurazione ISE).

```

12102  Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as
negotiated
12800  Extracted first TLS record; TLS handshake started
12805  Extracted TLS ClientHello message
12806  Prepared TLS ServerHello message

```



**12807 Prepared TLS Certificate message**  
**12809 Prepared TLS CertificateRequest message**  
 12105 Prepared EAP-Request with another EAP-FAST challenge  
 11006 Returned RADIUS Access-Challenge  
 11001 Received RADIUS Access-Request  
  
**12816 TLS handshake succeeded**  
 12207 **Client certificate was requested but not received during tunnel establishment. Will renegotiate and request client certificate inside the tunnel.**  
 12226 Started renegotiated TLS handshake  
  
 12104 Extracted EAP-Response containing EAP-FAST challenge-response  
**12811 Extracted TLS Certificate message containing client certificate**  
 12812 Extracted TLS ClientKeyExchange message  
 12804 Extracted TLS Finished message  
 12801 Prepared TLS ChangeCipherSpec message  
 12802 Prepared TLS Finished message  
 12226 Started renegotiated TLS handshake  
**12205 Client certificate was requested but not received inside the tunnel. Will continue with inner method.**  
**12149 EAP-FAST built authenticated tunnel for purpose of PAC provisioning**  
 12105 Prepared EAP-Request with another EAP-FAST challenge  
 11006 Returned RADIUS Access-Challenge  
 11001 Received RADIUS Access-Request  
 11018 RADIUS is re-using an existing session  
 12104 Extracted EAP-Response containing EAP-FAST challenge-response  
**12209 Starting EAP chaining**  
**12218 Selected identity type 'User'**  
**11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge**  
  
**24402 User authentication against Active Directory succeeded - example.com**  
**22037 Authentication Passed**  
  
**12126 EAP-FAST cryptobinding verification passed**  
 12200 Approved EAP-FAST client Tunnel PAC request  
 12202 Approved EAP-FAST client Authorization PAC request  
**12219 Selected identity type 'Machine'**  
  
**11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge**  
  
**24470 Machine authentication against Active Directory is successful - example.com**  
**22037 Authentication Passed**  
  
**12169 Successfully finished EAP-FAST tunnel PAC provisioning/update**  
**12171 Successfully finished EAP-FAST user authorization PAC provisioning/update**  
**12170 Successfully finished EAP-FAST machine PAC provisioning/update**  
**12179 Successfully finished EAP-FAST machine authorization PAC provisioning/update**  
  
 11503 Prepared EAP-Success  
 11002 Returned RADIUS Access-Accept

## EAP-Fast con concatenamento EAP e provisioning PAC tunnel TLS anonimo

In questo flusso, il tunnel TLS anonimo ISE e NAM è configurato per la preparazione PAC (il tunnel TLS autenticato ISE per la preparazione PAC è disabilitato) La richiesta di preparazione PAC ha il seguente aspetto:

- Il richiedente invia Hello al client TLS senza più suite di cifratura.
- Il server risponde con i cifrari TLS Server Hello e TLS anonimi Diffie Hellman (ad esempio

TLS\_DH\_anon\_WITH\_AES\_128\_CBC\_SHA).

- Il richiedente lo accetta e viene creato il tunnel TLS anonimo (nessun certificato scambiato).
- Avvia Concatenamento EAP per l'utente, utilizzando il metodo interno con l'autenticazione MSCHAPv2.
- Continua con l'autenticazione del computer, utilizzando il metodo interno con l'autenticazione MSCHAPv2.
- Poiché è in corso la creazione del tunnel TLS anonimo, le PAC di autorizzazione non sono consentite.
- Rifiuto Radius viene restituito per forzare il supplicant a riautenticarsi (utilizzando PAC con provisioning).

```
12102      Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST
as negotiated
12800      Extracted first TLS record; TLS handshake started
12805      Extracted TLS ClientHello message
12806      Prepared TLS ServerHello message
12808      Prepared TLS ServerKeyExchange message
12810      Prepared TLS ServerDone message

12812      Extracted TLS ClientKeyExchange message
12804      Extracted TLS Finished message
12801      Prepared TLS ChangeCipherSpec message
12802      Prepared TLS Finished message
12816      TLS handshake succeeded
12131      EAP-FAST built anonymous tunnel for purpose of PAC provisioning

12209      Starting EAP chaining
12218      Selected identity type 'User'

11806      Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge

24402      User authentication against Active Directory succeeded - example.com
22037      Authentication Passed

12162      Cannot provision Authorization PAC on anonymous provisioning. Authorization PAC can be
provisioned only on authenticated provisioning
12200      Approved EAP-FAST client Tunnel PAC request
12219      Selected identity type 'Machine'

24470      Machine authentication against Active Directory is successful - example.com
22037      Authentication Passed

12162      Cannot provision Authorization PAC on anonymous provisioning. Authorization PAC can be
provisioned only on authenticated provisioning
12169      Successfully finished EAP-FAST tunnel PAC provisioning/update
12170      Successfully finished EAP-FAST machine PAC provisioning/update

11504      Prepared EAP-Failure
11003      Returned RADIUS Access-Reject
```

Wireshark acquisisce i pacchetti per la negoziazione anonima del tunnel TLS:

Source	Destination	Protocol	Length	Info	User-Name
10.62.148.109	10.48.17.14	RADIUS	301	Access-Request(1) (id=190,	anonymous
10.48.17.14	10.62.148.109	RADIUS	193	Access-Challenge(11) (id=19	
10.62.148.109	10.48.17.14	RADIUS	498	Access-Request(1) (id=191,	anonymous
10.48.17.14	10.62.148.109	RADIUS	793	Access-Challenge(11) (id=19	
10.62.148.109	10.48.17.14	RADIUS	706	Access-Request(1) (id=192,	anonymous
10.48.17.14	10.62.148.109	RADIUS	232	Access-Challenge(11) (id=19	
10.62.148.109	10.48.17.14	RADIUS	378	Access-Request(1) (id=193,	anonymous
10.48.17.14	10.62.148.109	RADIUS	226	Access-Challenge(11) (id=19	
10.62.148.109	10.48.17.14	RADIUS	468	Access-Request(1) (id=194,	anonymous
10.48.17.14	10.62.148.109	RADIUS	258	Access-Challenge(11) (id=19	

Code: Request (1)

Id: 161

Length: 622

Type: Flexible Authentication via Secure Tunneling EAP (EAP-FAST) (43)

▷ EAP-TLS Flags: 0x01

▽ Secure Sockets Layer

▽ TLSv1 Record Layer: Handshake Protocol: Server Hello

Content Type: Handshake (22)

Version: TLS 1.0 (0x0301)

Length: 74

▽ Handshake Protocol: Server Hello

Handshake Type: Server Hello (2)

Length: 70

Version: TLS 1.0 (0x0301)

▷ Random

Session ID Length: 32

Session ID: 41aee5db065f48165c56144aa9dccdc93f67167fbae96393...

Cipher Suite: TLS\_DH\_anon\_WITH\_AES\_128\_CBC\_SHA (0x0034)

Compression Method: null (0)

▽ TLSv1 Record Layer: Handshake Protocol: Server Key Exchange

Content Type: Handshake (22)

## EAP-Fast con solo autenticazione utente concatenamento EAP

In questo flusso, viene configurato AnyConnect NAM con EAP-FAST e autenticazione utente (EAP-TLS) e computer (EAP-TLS). Il PC Windows è stato avviato ma non sono state fornite le credenziali utente. Lo switch avvia la sessione 802.1x, NAM deve rispondere ma le credenziali utente non sono fornite (non è ancora possibile accedere all'archivio utenti e al certificato). L'autenticazione dell'utente avrà esito negativo se il computer avrà esito positivo. La condizione di autorizzazione ISE "Accesso di rete:EapChainingResult EQUALS Utente non riuscito e computer riuscito" è soddisfatta. In seguito, l'utente eseguirà l'accesso e verrà avviata un'altra autenticazione, sia per l'utente che per il computer.

- Il richiedente invia al client TLS Hello con PAC computer.
- Il server risponde con la specifica di crittografia TLS - il tunnel TLS viene immediatamente creato in base a tale PAC.
- ISE avvia EAP Chaining e richiede l'identità dell'utente.

- Supplicant fornisce invece l'identità del computer (utente non ancora pronto) e completa il metodo interno EAP-TLS.
- ISE richiede nuovamente l'identità dell'utente, il richiedente non può fornirla.
- ISE invia TLV con risultato intermedio = errore (per l'autenticazione dell'utente).
- ISE restituisce il messaggio di riuscita EAP finale. La condizione ISE Accesso di rete:EapChainingResult EQUALS Utente non riuscito e computer riuscito è soddisfatto.

```

12102  Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as
negotiated
12800  Extracted first TLS record; TLS handshake started
12174  Received Machine PAC

12805  Extracted TLS ClientHello message
12806  Prepared TLS ServerHello message
12801  Prepared TLS ChangeCipherSpec message
12802  Prepared TLS Finished message

12816  TLS handshake succeeded
12132  EAP-FAST built PAC-based tunnel for purpose of authentication

12209  Starting EAP chaining
12218  Selected identity type 'User'

12213  Identity type provided by client is not equal to requested type
12215  Client suggested 'Machine' identity type instead

12104  Extracted EAP-Response containing EAP-FAST challenge-response
12523  Extracted EAP-Response/NAK for inner method requesting to use EAP-TLS instead

12805  Extracted TLS ClientHello message
12806  Prepared TLS ServerHello message
12807  Prepared TLS Certificate message
12809  Prepared TLS CertificateRequest message

12816  TLS handshake succeeded
12509  EAP-TLS full handshake finished successfully

22070  Identity name is taken from certificate attribute
15013  Selected Identity Source - Test-AD
24323  Identity resolution detected single matching account
22037  Authentication Passed

12202  Approved EAP-FAST client Authorization PAC request
12218  Selected identity type 'User'
12213  Identity type provided by client is not equal to requested type
12216  Identity type provided by client was already used for authentication
12967  Sent EAP Intermediate Result TLV indicating failure

12179  Successfully finished EAP-FAST machine authorization PAC provisioning/update
12106  EAP-FAST authentication phase finished successfully
11503  Prepared EAP-Success
11002  Returned RADIUS Access-Accept

```

## EAP-Fast con concatenamento EAP e impostazioni del tunnel TLS anonimo incoerenti

In questo flusso, ISE è configurato per la preparazione della PAC solo tramite un tunnel TLS anonimo, ma NAM utilizza un tunnel TLS autenticato. ISE registrerà quanto segue:

```
12102  Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as
negotiated
12800  Extracted first TLS record; TLS handshake started
12805  Extracted TLS ClientHello message
12814  Prepared TLS Alert message
12817  TLS handshake failed
12121  Client didn't provide suitable ciphers for anonymous PAC-provisioning

11504  Prepared EAP-Failure
11003  Returned RADIUS Access-Reject
```

Questo si verifica quando NAM sta tentando di costruire un tunnel TLS autenticato con i suoi cifrari TLS specifici - e questi non sono accettati da ISE, che è configurato per il tunnel TLS anonimo (accetta solo cifrari DH)

## Risoluzione dei problemi

### ISE

Per i registri dettagliati, è necessario abilitare i debug Runtime-AAA sul nodo PSN corrispondente. Di seguito sono riportati alcuni log di esempio da port-server.log:

#### Generazione PAC computer:

```
DEBUG,0x7fd5332fe700,cntx=0001162745,sesn=mgarcarz-
ise14/223983918/29245,CPMSessionID=0A3E946D0000FE5131F9D26,CallingStationID=00-50-B6-11-ED-
31,FramedIPAddress=10.0.13.127,Using IID from PAC request for machine,EapFastTlv.cpp:1234

DEBUG,0x7fd5332fe700,cntx=0001162745,sesn=mgarcarz-
ise14/223983918/29245,CPMSessionID=0A3E946D0000FE5131F9D26,CallingStationID=00-50-B6-11-ED-
31,FramedIPAddress=10.0.13.127,Adding PAC of type=Machine Authorization,EapFastProtocol.cpp:3610

DEBUG,0x7fd5332fe700,cntx=0001162745,sesn=mgarcarz-
ise14/223983918/29245,CPMSessionID=0A3E946D0000FE5131F9D26,CallingStationID=00-50-B6-11-ED-
31,FramedIPAddress=10.0.13.127,Eap-Fast: Generating Pac, Issued PAC type=Machine Authorization
with expiration time: Fri Jul 3 10:38:30 2015
```

#### Approvazione richiesta PAC:

```
INFO ,0x7fd5330fc700,cntx=0001162745,sesn=mgarcarz-
ise14/223983918/29245,CPMSessionID=0A3E946D0000FE5131F9D26,user=host/mgarcarz-
pc,CallingStationID=00-50-B6-11-ED-31,FramedIPAddress=10.0.13.127,Eap-Fast: client PAC request
approved for PAC type - Requested PAC type=Machine,EapFastProtocol.cpp:955

INFO ,0x7fd5330fc700,cntx=0001162745,sesn=mgarcarz-
ise14/223983918/29245,CPMSessionID=0A3E946D0000FE5131F9D26,user=host/mgarcarz-
pc,CallingStationID=00-50-B6-11-ED-31,FramedIPAddress=10.0.13.127,Eap-Fast: client PAC request
approved for PAC type - Requested PAC type=Machine Authorization,EapFastProtocol.cpp:955
```

#### Convalida PAC:

```
DEBUG,0x7fd5330fc700,cntx=0001162499,sesn=mgarcarz-
ise14/223983918/29243,CPMSessionID=0A3E946D0000FE5131F9D26,user=anonymous,CallingStationID=00-
50-B6-11-ED-31,FramedIPAddress=10.0.13.127,Authorization PAC is valid,EapFastProtocol.cpp:3403
```

```
Eap,2015-07-03 09:34:39,208,DEBUG,0x7fd5330fc700,cntx=0001162499,sesn=mgarcarz-ise14/223983918/29243,CPMSessionID=0A3E946D00000FE5131F9D26,user=anonymous,CallingStationID=00-50-B6-11-ED-31,FramedIPAddress=10.0.13.127,Authorization PAC accepted,EapFastProtocol.cpp:3430
```

Esempio di riepilogo corretto per la generazione della PAC:

```
DEBUG,0x7fd5331fd700,cntx=0001162749,sesn=mgarcarz-ise14/223983918/29245,CPMSessionID=0A3E946D00000FE5131F9D26,user=cisco,CallingStationID=00-50-B6-11-ED-31,FramedIPAddress=10.0.13.127,Conversation summary: Provisioning. Authenticated. Inner method succeeded. Inner method succeeded. Generated PAC of type Tunnel V1A. Generated PAC of type User Authorization. Generated PAC of type Machine. Generated PAC of type Machine Authorization. Success
```

Esempio di riepilogo corretto per la convalida della PAC:

```
DEBUG,0x7fd5330fc700,cntx=0001162503,sesn=mgarcarz-ise14/223983918/29243,CPMSessionID=0A3E946D00000FE5131F9D26,user=host/mgarcarz-pc,CallingStationID=00-50-B6-11-ED-31,FramedIPAddress=10.0.13.127,Conversation summary: Authentication. PAC type Tunnel V1A. PAC is valid.Skip inner method. Skip inner method. Success
```

## AnyConnect NAM

I registri DART di NAM forniscono i dettagli seguenti:

Esempio di sessione senza concatenamento EAP, autenticazione del computer senza riconnessione rapida:

```
EAP: Identity requested  
Auth[eap-fast-pac:machine-auth]: Performing full authentication  
Auth[eap-fast-pac:machine-auth]: Disabling fast reauthentication
```

Esempio di ricerca nella PAC di autorizzazione (autenticazione computer per sessione non EAP-Chaining):

```
Looking for matching pac with iid: host/ADMIN-PC2  
Requested machine pac was sen
```

Tutti gli stati del metodo interno (per MSCHAP) possono essere verificati dai seguenti registri:

```
EAP (0) EAP-MSCHAP-V2: State: 0 (eap_auth_mschapv2_c.c 731  
EAP (0) EAP-MSCHAP-V2: State: 2 (eap_auth_mschapv2_c.c 731  
EAP (0) EAP-MSCHAP-V2: State: 1 (eap_auth_mschapv2_c.c 731  
EAP (0) EAP-MSCHAP-V2: State: 4 (eap_auth_mschapv2_c.c 73
```

NAM consente la configurazione della funzione di registrazione estesa che acquisirà tutti i pacchetti EAP e li salverà nel file PCAP. Ciò è particolarmente utile per la funzionalità Avvia prima dell'accesso (i pacchetti EAP vengono acquisiti anche per le autenticazioni eseguite prima dell'accesso dell'utente). Per informazioni sull'attivazione delle caratteristiche, rivolgersi al tecnico TAC.

## Riferimenti

- [Guida per l'amministratore di Cisco AnyConnect Secure Mobility Client, configurazione EAP-FAST versione 4.0](#)

- [Guida per l'amministratore di Cisco Identity Services Engine, release 1.4 - Consigli per EAP-FAST](#)
- [Guide alla progettazione di Cisco Identity Services Engine](#)
- [Implementazione del concatenamento EAP con AnyConnect NAM e Cisco ISE](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)