Cisco Secure Services Client con autenticazione EAP-FAST

Sommario

Introduzione **Prerequisiti** Requisito Componenti usati Convenzioni Parametri di progettazione Database Crittografia Single Sign-on e credenziali del computer Esempio di rete Configurazione di Access Control Server (ACS) Aggiunta di un punto di accesso come client AAA (NAS) in ACS Configurazione di ACS per eseguire guery sul database esterno Abilita supporto EAP-FAST su ACS **Controller WLAN Cisco** Configurazione del controller LAN wireless Funzionamento di base e registrazione dei LAP sul controller Autenticazione RADIUS tramite Cisco Secure ACS Configurazione dei parametri WLAN Verifica operazione Appendice Acquisizione sniffer per Exchange EAP-FAST Debug sul controller WLAN Informazioni correlate

Introduzione

In questo documento viene descritto come configurare Cisco Secure Services Client (CSSC) con i controller LAN wireless, il software Microsoft Windows 2000[®] e Cisco Secure Access Control Server (ACS) 4.0 con EAP-FAST. Questo documento introduce l'architettura EAP-FAST e fornisce esempi di distribuzione e configurazione. CSSC è il componente software del client che fornisce la comunicazione delle credenziali utente all'infrastruttura per autenticare un utente alla rete e assegnare l'accesso appropriato.

Di seguito sono riportati alcuni dei vantaggi della soluzione CSSC evidenziati in questo documento:

- Autenticazione di ciascun utente (o dispositivo) prima dell'autorizzazione di accesso alla WLAN/LAN con EAP (Extensible Authentication Protocol)
- Soluzione completa per la sicurezza WLAN con server, autenticatore e componenti client
- Soluzione comune per l'autenticazione cablata e wireless
- Chiavi di crittografia dinamiche per utente derivate nel processo di autenticazione
- Nessun requisito per infrastruttura a chiave pubblica (PKI) o certificati (verifica certificato facoltativa)
- Assegnazione dei criteri di accesso e/o framework EAP abilitato per NAC

Nota: per informazioni sull'implementazione di una tecnologia wireless sicura, consultare il <u>Cisco</u> <u>SAFE Wireless Blueprint</u>.

Il framework di autenticazione 802.1x è stato incorporato come parte dello standard 802.11i (Wireless LAN Security) per abilitare le funzioni di autenticazione, autorizzazione e accounting basate sul layer 2 in una rete LAN wireless 802.11. Attualmente sono disponibili diversi protocolli EAP per l'installazione in reti cablate e wireless. I protocolli EAP comunemente implementati includono LEAP, PEAP e EAP-TLS. Oltre a questi protocolli, Cisco ha definito e implementato il protocollo EAP (EAP-FAST) per l'autenticazione flessibile EAP tramite tunnel protetto come protocollo EAP basato su standard, disponibile per l'installazione su reti LAN cablate e wireless. La specifica del protocollo EAP-FAST è disponibile al pubblico sul <u>sito Web</u> dell'<u>IETF</u>.

Come altri protocolli EAP, EAP-FAST è un'architettura di sicurezza client-server che cripta le transazioni EAP all'interno di un tunnel TLS. Anche se simile a PEAP o EAP-TTLS in questo senso, differisce in quanto la creazione del tunnel EAP-FAST si basa su chiavi segrete condivise sicure che sono univoche per ogni utente, rispetto a PEAP/EAP-TTLS (che usano un certificato X.509 del server per proteggere la sessione di autenticazione). Queste chiavi segrete condivise sono denominate credenziali di accesso protette (PAC) e possono essere distribuite automaticamente (provisioning automatico o in banda) o manualmente (provisioning manuale o fuori banda) ai dispositivi client. Poiché gli handshake basati su segreti condivisi sono più efficienti degli handshake basati su un'infrastruttura PKI, EAP-FAST è il tipo di EAP più veloce e meno intensivo per il processore tra quelli che forniscono scambi di autenticazione protetti. EAP-FAST è progettato anche per la semplicità di implementazione, in quanto non richiede un certificato sul client LAN wireless o sull'infrastruttura RADIUS ma incorpora un meccanismo di provisioning integrato.

Di seguito sono riportate alcune delle principali funzionalità del protocollo EAP-FAST:

- Single Sign-On (SSO) con nome utente/password di Windows
- Supporto per l'esecuzione dello script di accesso
- Supporto Wi-Fi Protected Access (WPA) senza supporto di terze parti (solo Windows 2000 e XP)
- Installazione semplice senza necessità di infrastruttura PKI
- Scadenzario password di Windows (supporto per la scadenza delle password basata su server)
- Integrazione con Cisco Trust Agent per Network Admission Control con il software client appropriato

Prerequisiti

Requisito

Si presume che il programma di installazione conosca le procedure di base per l'installazione di Windows 2003 e di Cisco WLC, in quanto nel presente documento vengono descritte solo le configurazioni specifiche per semplificare i test.

Per informazioni sull'installazione iniziale e sulla configurazione dei Cisco serie 4400 Controller, fare riferimento alla <u>Guida introduttiva: Cisco serie 4400 Wireless LAN Controller</u>. Per informazioni sull'installazione iniziale e sulla configurazione dei Cisco serie 2000 Controller, fare riferimento alla <u>Guida introduttiva: Cisco serie 2000 Wireless LAN Controller</u>.

Prima di iniziare, installare Microsoft Windows Server 2000 con il Service Pack più recente. Installare i controller e i Lightweight Access Point (LAP) e verificare che siano configurati gli ultimi aggiornamenti software.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Controller Cisco serie 2006 o 4400 con 4.0.155.5
- Cisco 1242 LWAPP AP AP
- Windows 2000 con Active Directory
- Cisco Catalyst 3750G Switch
- Windows XP con scheda adattatore CB21AG e Cisco Secure Services Client versione 4.05

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento <u>Cisco sulle convenzioni</u> <u>nei suggerimenti tecnici.</u>

Parametri di progettazione

Database

Quando si distribuisce una rete WLAN e si cerca un protocollo di autenticazione, in genere si desidera utilizzare un database corrente per l'autenticazione utente/computer. I database tipicamente utilizzabili sono Windows Active Directory, LDAP o OTP (One Time Password), ovvero RSA o SecureID. Tutti questi database sono compatibili con il protocollo EAP-FAST, ma quando si pianifica la distribuzione, è necessario considerare alcuni requisiti di compatibilità. La distribuzione iniziale di un file PAC ai client viene eseguita tramite la preparazione automatica anonima, la preparazione autenticata (tramite il certificato X.509 del client corrente) o la preparazione manuale. Ai fini del presente documento, vengono presi in considerazione l'autoprovisioning anonimo e il provisioning manuale.

La preparazione automatica delle credenziali di accesso protette utilizza il protocollo ADHP (Authenticated Diffie-Hellman Key Agreement Protocol) per stabilire un tunnel sicuro. Il tunnel sicuro può essere stabilito in modo anonimo o tramite un meccanismo di autenticazione server. All'interno della connessione del tunnel stabilita, MS-CHAPv2 viene utilizzato per autenticare il client e, se l'autenticazione ha esito positivo, per distribuire il file PAC al client. Una volta completato il provisioning della PAC, è possibile utilizzare il file PAC per avviare una nuova sessione di autenticazione EAP-FAST al fine di ottenere un accesso sicuro alla rete.

La preparazione automatica della PAC è rilevante per il database in uso poiché, poiché il meccanismo di preparazione automatica si basa su MSCHAPv2, il database utilizzato per autenticare gli utenti deve essere compatibile con questo formato della password. Se si utilizza EAP-FAST con un database che non supporta il formato MSCHAPv2 (ad esempio OTP, Novell o LDAP), è necessario utilizzare un altro meccanismo (ovvero la preparazione manuale o la preparazione autenticata) per distribuire i file PAC utente. In questo documento viene illustrato un esempio di provisioning automatico con un database utenti di Windows.

Crittografia

L'autenticazione EAP-FAST non richiede l'utilizzo di un tipo di crittografia WLAN specifico. Il tipo di crittografia WLAN da utilizzare è determinato dalle funzionalità della scheda NIC del client. Si consiglia di utilizzare la crittografia WPA2 (AES-CCM) o WPA(TKIP), a seconda delle funzionalità della scheda NIC nell'implementazione specifica. La soluzione Cisco WLAN consente la coesistenza di dispositivi client WPA2 e WPA su un SSID comune.

Se i dispositivi client non supportano WPA2 o WPA, è possibile implementare l'autenticazione 802.1X con chiavi WEP dinamiche, ma, a causa di attacchi noti alle chiavi WEP, questo meccanismo di crittografia WLAN non è consigliato. Se è necessario supportare client solo WEP, si consiglia di utilizzare un intervallo di timeout della sessione, che richiede che i client derivino una nuova chiave WEP a intervalli frequenti. L'intervallo di sessione consigliato è di 30 minuti per le velocità dati tipiche della WLAN.

Single Sign-on e credenziali del computer

Il termine Single Sign-On si riferisce alla capacità di un singolo accesso utente o di un'immissione di credenziali di autenticazione da utilizzare per accedere a più applicazioni o dispositivi. Ai fini del presente documento, per Single Sign-On si intende l'utilizzo delle credenziali utilizzate per accedere a un PC per l'autenticazione alla WLAN.

Con Cisco Secure Services Client, è possibile usare le credenziali di accesso di un utente anche per autenticarsi alla rete WLAN. Se si desidera autenticare un PC per la rete prima che l'utente acceda al PC, è necessario utilizzare le credenziali utente archiviate o le credenziali associate a un profilo del computer. Entrambi i metodi sono utili nei casi in cui si desidera eseguire script di accesso o mappare le unità all'avvio del PC, anziché all'accesso dell'utente.

Esempio di rete

Questo è il diagramma di rete usato nel documento. In questa rete vengono utilizzate quattro subnet. Non è necessario segmentare questi dispositivi in diverse reti, ma questa operazione offre la massima flessibilità per l'integrazione con le reti reali. Il controller LAN wireless integrato Catalyst 3750G fornisce porte di switching Power Over Ethernet (POE), switching L3 e funzionalità del controller WLAN su uno chassis comune.

- 1. La rete 10.1.1.0 è la rete del server in cui risiede l'ACS.
- 2. La rete 10.10.80.0 è la rete di gestione usata dal controller WLAN.
- 3. La rete 10.10.81.0 è la rete in cui risiedono gli access point.
- 4. Per i client WLAN viene utilizzata la rete 10.10.82.0.



Configurazione di Access Control Server (ACS)

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo <u>strumento di</u> <u>ricerca</u> dei comandi (solo utenti <u>registrati</u>).

Aggiunta di un punto di accesso come client AAA (NAS) in ACS

In questa sezione viene descritto come configurare ACS per EAP-FAST con la preparazione della PAC in banda con Windows Active Directory come database esterno.

- 1. Accedere a ACS > Network Configuration (Configurazione di rete) e fare clic su Add Entry (Aggiungi voce).
- 2. Specificare il nome del controller WLAN, l'indirizzo IP, la chiave segreta condivisa e in Autenticazione tramite scegliere RADIUS (Cisco Airespace), che include anche gli attributi IETF RADIUS.Nota: Se i gruppi di dispositivi di rete (NDG) sono abilitati, scegliere il NDG appropriato e aggiungervi il controller WLAN. Per ulteriori informazioni su NDG, consultare la guida alla configurazione di ACS.
- 3. Fare clic su **Submit+** Restart.

Cisco Systems	Network Configuration				
	Edit				
User Setup					
Group Setup	AAA Client Setup For				
SharedProfile Components	ws-3750				
Network Configuration	10.10.80.3				
System Configuration	AAA Client IP Address				
Configuration	Key cisco123				
Administration Control	Authenticate Using RADIUS (Cisco Airespace)				
Databases	Single Connect TACACS+ AAA Client (Record stop in accounting on failure).				
Posture Validation	Log Update/Watchdog Packets from this AAA Client				
Network Access	Log RADIUS Tunneling Packets from this AAA Client				
I Reports and	Replace RADIUS Port info with Username from this AAA Client				
Activity					
Documentation	Submit Submit + Apply Delete Delete + Apply Cancel				
	💡 Back to Help				

Configurazione di ACS per eseguire query sul database esterno

In questa sezione viene descritto come configurare ACS per eseguire query sul database esterno.

- 1. Fare clic su Database utente esterno > Configurazione database > Database di Windows > Configura.
- 2. In Configura elenco domini spostare i domini da Domini disponibili a Elenco domini.Nota: affinché l'applicazione ACS possa rilevare e utilizzare i domini per l'autenticazione, è necessario che il server che esegue ACS conosca questi domini.



- 3. In Impostazioni EAP Windows configurare l'opzione per consentire la modifica della password nella sessione PEAP o EAP-FAST. Per ulteriori informazioni su EAP-FAST e sulla durata delle password di Windows, consultare la guida alla configurazione di Cisco Secure ACS 4.1.
- 4. Fare clic su Invia. Nota: è inoltre possibile attivare la funzionalità Autorizzazione chiamata per EAP-FAST in Configurazione database utenti di Windows per consentire al database esterno di Windows di controllare le autorizzazioni di accesso. Le impostazioni MS-CHAP per la modifica della password nella pagina di configurazione del database di Windows sono applicabili solo all'autenticazione MS-CHAP non EAP. Per attivare la modifica della password in combinazione con EAP-FAST, è necessario attivare la modifica della password in Impostazioni EAP di

Windows.



	a	
ser etup	Windows EAP Settings 💡	1
	Enable password change inside PEAP or EAP-FAST.	
file	EAP-TLS Strip Domain Name.	
Ma	chine Authentication.	
	Enable PEAP machine authentication.	
	Enable EAP-TLS machine authentication.	
	EAP-TLS and PEAP machine authentication name host/	
	Enable machine access restrictions.	
	Aging time (hours): 12	
	Group map for successful user authentication without (No Access)	
	User Groups that are exempt from passing machine authentication:	
	Available User Groups Selected User Groups	
	Oroup 1	
	Group 2	
	Group 4 <-	
	Group 6	
	Group 7 Group 8	
Tł	ese settings can be used to enable or disable specific Windows EAP functionality	-
		=
	Submit Cancel	

- 5. Fare clic su **Database utenti esterni > Criterio utente sconosciuto** e scegliere il pulsante di opzione **Controlla i seguenti database utenti esterni**.
- 6. Spostare il database di Windows dai database esterni ai database selezionati.
- 7. Fare clic su Invia.Nota: da questo punto in poi, ACS controlla il database di Windows. Se l'utente non viene trovato nel database locale ACS, viene inserito nel gruppo predefinito ACS. Per ulteriori informazioni sui mapping dei gruppi di database, consultare la documentazione di ACS.Nota: poiché ACS esegue query sul database di Microsoft Active Directory per verificare le credenziali utente, è necessario configurare in Windows ulteriori impostazioni relative ai diritti di accesso. Per ulteriori informazioni, consultare la Guida all'installazione di Cisco Secure ACS per Windows Server.



Abilita supporto EAP-FAST su ACS

In questa sezione viene descritto come abilitare il supporto EAP-FAST sul server ACS.

- 1. Selezionare Configurazione di sistema > Impostazione autenticazione globale > Configurazione EAP-FAST.
- 2. Scegliere Consenti EAP-FAST.
- 3. Configurare i suggerimenti seguenti: TTL chiave master/TTL chiave master ritirata/TTL PAC. Queste impostazioni sono configurate per impostazione predefinita in Cisco Secure ACS:TTL: 1 mese chiave masterTTL chiave ritirata: 3 mesiTTL PAC: 1 settimana
- 4. Compilare il campo **Informazioni sull'ID autorità**. Questo testo viene visualizzato su alcuni software client EAP-FAST in cui la selezione dell'autorità PAC è il controller.**Nota:** Cisco Secure Services Client non utilizza questo testo descrittivo per l'autorità PAC.
- 5. Scegliere il campo **Consenti preparazione PAC in banda**. Questo campo abilita la preparazione automatica della PAC per i client EAP-FAST abilitati correttamente. Per questo esempio, viene utilizzato il provisioning automatico.
- 6. Scegliere i metodi interni consentiti: EAP-GTC e EAP-MSCHAP2. Ciò consente il funzionamento di client EAP-FAST v1 e EAP-FAST v1a. (Cisco Secure Services Client supporta EAP-FAST v1a). Se non è necessario supportare i client EAP-FAST v1, è necessario abilitare EAP-MSCHAPv2 solo come metodo interno.
- 7. Selezionare la casella di controllo EAP-FAST Master Server per abilitare il server EAP-FAST

come master. Questo consente agli altri server ACS di utilizzare il server come autorità PAC master per evitare di fornire chiavi univoche per ciascun ACS di una rete. Per ulteriori informazioni, consultare la guida alla configurazione di ACS.

8. Fare clic su

Invia+Riavvia.

Cisco	SYSTEMS	
ah	ւսև	

System Configuration

	Aor comgaration
EA	P-FAST Settings
Active master key TTL	1 months 💌
Retired master key TTL	3 months 💌
Tunnel PAC TTL	1 weeks 💌
Client initial message:	TME
Authority ID Info:	TME
Allow anonymous in-band PAC	provisioning
Allow authenticated in-band P	AC provisioning
Accept client on authentic	ated provisioning
Require client certificate fo	or provisioning
Allow Machine Authentication	
Machine PAC TTL	1 weeks 🛩
Allow Stateless session resume	3
Authorization PAC TTL	1 hours 💌
Allowed inner methods	
EAP-GTC	
EAP-MSCHAPv2	
EAP-TLS	
Select one or more of the following	ng EAP-TLS comparison methods:
Certificate SAN comparisor	1
Certificate CN comparison	
Certificate Binary comparis	on
EAP-TLS session timeout (minute	s) 120
EAP-FAST master server	
Actual EAP-FAST server status	Master

EAP-FAST Configuration

Controller WLAN Cisco

Ai fini della presente Guida alla distribuzione, un Cisco WS3750G Integrated Wireless LAN Controller (WLC) viene utilizzato con i Cisco AP1240 Lightweight AP (LAP) per fornire l'infrastruttura WLAN per i test CSSC. la configurazione è applicabile a tutti i controller WLAN Cisco. La versione software utilizzata è la 4.0.155.5.

Configurazione del controller LAN wireless

Funzionamento di base e registrazione dei LAP sul controller

Per configurare il WLC per il funzionamento di base, usare la configurazione guidata di avvio sull'interfaccia della riga di comando (CLI). In alternativa, è possibile usare la GUI per configurare il WLC. Questo documento spiega la configurazione sul WLC con la configurazione guidata di avvio sulla CLI.

Una volta avviato per la prima volta, il WLC entra nella configurazione guidata di avvio. Utilizzare la configurazione guidata per configurare le impostazioni di base. È possibile accedere alla procedura guidata dalla CLI o dalla GUI. Questo output mostra un esempio della configurazione guidata di avvio nella CLI:

Welcome to the Cisco Wizard Configuration Tool Use the '-' character to backup System Name [Cisco 33:84:a0]: ws-3750 Enter Administrative User Name (24 characters max): admin Enter Administrative Password (24 characters max): ***** Management Interface IP Address: 10.10.80.3 Management Interface Netmask: 255.255.255.0 Management Interface Default Router: 10.10.80.2 Management Interface VLAN Identifier (0 = untagged): Management Interface DHCP Server IP Address: 10.10.80.2 AP Manager Interface IP Address: 10.10.80.4 AP-Manager is on Management subnet, using same values AP Manager Interface DHCP Server (172.16.1.1): Virtual Gateway IP Address: 1.1.1.1 Mobility/RF Group Name: Security Network Name (SSID): Enterprise Allow Static IP Addresses [YES][no]: yes Configure a RADIUS Server now? [YES][no]: no Warning! The default WLAN security policy requires a RADIUS server. Please see documentation for more details. Enter Country Code (enter 'help' for a list of countries) [US]: Enable 802.11b Network [YES][no]: yes Enable 802.11a Network [YES][no]: yes Enable 802.11g Network [YES][no]: yes Enable Auto-RF [YES][no]: yes Configuration saved! Resetting system with new configuration.

Questi parametri configurano il WLC per il funzionamento di base. Nella configurazione di esempio, il WLC usa **10.10.80.3** come indirizzo IP dell'interfaccia di gestione e **10.10.80.4** come indirizzo IP dell'interfaccia del gestore dell'access point.

Prima di poter configurare altre funzionalità sui WLC, i LAP devono registrarsi sul WLC. per le successive spiegazioni, si presume che il LAP sia registrato sul WLC. Per informazioni su come i Lightweight Access Point si registrano sul WLC, fare riferimento alla sezione <u>Registrazione</u> del Lightweight AP sui <u>WLC</u> di <u>esempio di configurazione del failover dei WLAN Controller per Lightweight Access Point</u>. Per riferimento a questo esempio di configurazione, gli AP1240 vengono distribuiti su una subnet separata (10.10.81.0/24) dal controller WLAN (10.10.80.0/24) e l'opzione DHCP 43 viene utilizzata per rilevare i controller.

Autenticazione RADIUS tramite Cisco Secure ACS

Ènecessario configurare il WLC per inoltrare le credenziali dell'utente al server Cisco Secure ACS.

Il server ACS convalida quindi le credenziali dell'utente (tramite il database di Windows configurato) e fornisce l'accesso ai client wireless.

Completare questa procedura per configurare il WLC per la comunicazione con il server ACS:

 Fare clic su Sicurezza e Autenticazione RADIUS dall'interfaccia utente del controller per visualizzare la pagina Server di autenticazione RADIUS. Quindi fare clic su New (Nuovo) per definire il server

ACS.		
Core Service		Save Configuration Ping Lagout Refresh
A. A.	MONITOR WLARE CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	
Security	RADIUS Authentication Servers	Apply New
AAA General	Call Station ID Type 17 Address 💌	
RADJUS Authenticetion RADJUS Accounting Lacel Net Users	Credentials Caching	
MAC Filtering Disabled Clients	Use AES Key Wrap	
AP Policies Access Control Lists	Network Nanagement Server Index Server Address Port IPSec Admin Status	
IPSec Certificates CA Certificate ID Certificate		

2. Definire i parametri del server ACS nella pagina Server di autenticazione RADIUS > Nuovo. Questi parametri includono l'indirizzo IP ACS, il segreto condiviso, il numero di porta e lo stato del server.**Nota:** i numeri di porta 1645 o 1812 sono compatibili con ACS per l'autenticazione RADIUS.Le caselle di controllo Utente e gestione rete determinano se l'autenticazione basata su RADIUS è valida per gli utenti di rete (ad esempio, i client WLAN) e per la gestione (ovvero, gli utenti amministrativi). Nella configurazione di esempio, il server RADIUS Cisco Secure ACS ha indirizzo IP

10.1.1.1Z:							
Come Stormer						Sale Configuration Pin	g Logout Refresh
A.A.	MONITOR WILLINS CONTR	OLLER WIRELESS SECURIT	IY NANAGEMENT	COMMANDS	HEUP		
Security	RADIUS Authentication Ser	vers > New				< Back	Apply
AAA General	Server Index (Priority)	1 💌					
RADIUS Authentication RADIUS Accounting Local Net Deers	Server IPAddress	10.1.1.12					
MAC Filtwing Disabled Chevis	Shared Secret Format	ASCII 💌					
AP Policies	Shared Secret	******					
Access Control Lists IPSec Certificates	Confirm Shared Secret	•••••					
ADDUS Authentication RADDUS Accounting	Berver IPAddress	10.1.1.12					
NAC Filturing Disabled Clients	Shared Secret Format	ASCII M					
AP Polisies	Shared Secret]		
Access Control Lists IPSec Certificates	Confirm Shared Secret	******			2		
CA Certificate ID Certificate	Key Wrap						
Web Auth Certificate Wireless Protection	Port Number	1812					
Trusted AP Palicies Rogae Policies	Server Status	Enabled 💌					
Standard Signatures Custom Signatures Signature Exerts	Support for RFC 3576	Enabled 💌					
Client Exclusion Policies AP Authentication / MFP	Retransmit Timeout	z seconds					
Nanagement Preme Protection	Network User	🗹 Enable					
Web Lagin Page	Management	Enable					
Sensore Shanned Clients	IPSec	Enable					

Configurazione dei parametri WLAN

40 4 4 40

In questa sezione viene descritta la configurazione di Cisco Secure Services Client. Nell'esempio, CSSC v4.0.5.4783 viene usato con una scheda client Cisco CB21AG. Prima di installare il software CSSC, verificare che siano installati solo i driver per CB21AG e non Aironet Desktop Utility (ADU).

Dopo aver installato il software e averlo eseguito come servizio, cerca le reti disponibili e le visualizza.

Nota: CSSC disabilita Windows Zero Config.

Nota: sono visibili solo i SSID abilitati per la trasmissione.

Cisco Secure Services Client	
Client Administration Help	
Lreate Networks Manage Networks	
Access 🔺	Data Security 📩
bigmonkey (2 accesses detected)	骨 WPA2
employee-local	🗃 WPA2
Enterprise (4 accesses detected)	PA2 VPA2
00141b5a2bd0 High Signal 00141b5a2bd(High Signal	WPA WPA
00141b5a33d0 Very High Signal	WPA
00141b5a33df High Signal	WPA
guest	🞽 Open
guest-central	🎽 Open 📃
guestnet (6 accesses detected)	🞽 Open
H-REAP_TEST_1	WEP
H-REAP_TEST_3	WEP
H-REAP_TEST_4	WEP
H-REAP_TEST_5	WEP
H-REAP_TEST_6	MEP
H-REAP_TEST_7	MEP ⊻
Create Network	

Nota: per impostazione predefinita, il controller WLAN trasmette l'SSID, quindi viene visualizzato nell'elenco Crea reti di SSID analizzati. Per creare un profilo di rete, è sufficiente fare clic sul **SSID** nella lista (Enterprise) e sul pulsante di opzione **Crea rete**.

Se l'infrastruttura WLAN è configurata con SSID broadcast disabilitato, è necessario aggiungere manualmente l'SSID; fare clic sul pulsante di scelta **Aggiungi** in Dispositivi di accesso e immettere manualmente il **SSID** appropriato (ad esempio, Enterprise). configurare il comportamento del probe attivo per il client, ovvero il client verifica attivamente il SSID configurato; specificare **Ricercare attivamente la periferica di accesso** dopo aver immesso il SSID nella finestra Aggiungi periferica di accesso.

Nota: le impostazioni della porta non consentono le modalità enterprise (802.1X) se le impostazioni di autenticazione EAP non sono configurate per il profilo.

Il pulsante di scelta **Crea rete** apre la finestra Profilo di rete, che consente di associare l'SSID scelto (o configurato) a un meccanismo di autenticazione. Assegnare un nome descrittivo per il profilo.

Nota: sotto questo profilo di autenticazione è possibile associare più tipi di sicurezza WLAN e/o SSID.

Per fare in modo che il client si connetta automaticamente alla rete quando si trova nel campo di copertura RF, scegliere **Stabilisci automaticamente connessione utente**. Deselezionare **Disponibile per tutti gli utenti** se non si desidera utilizzare questo profilo con altri account utente sul computer. Se non si sceglie **Stabilisci automaticamente**, è necessario che l'utente apra la finestra CSSC e avvii manualmente la connessione WLAN con il pulsante di opzione **Connetti**.

Se si desidera avviare la connessione WLAN prima dell'accesso dell'utente, scegliere **Prima dell'account utente**. Ciò consente l'operazione Single Sign-On con credenziali utente salvate (password o certificato/smart card quando si utilizza TLS in EAP-FAST).

The Network Profile	×				
Network Name: Enterprise Network Image: Available to all users (public profile) Image: Automatically establish Machine connection Image: Automatically establish User connection Image: Before user account (supports smartcard/password only)					
Network Configuration Summary:					
Authentication: FAST;					
Credentials: Request when needed and remember forever.					
Modify					
Access Devices	h				
Access / SSID Mode Notes					
Enterprise WPA2 Enterprise					
Add Modify Configuration Remove					
Help OK Cancel)				

Nota: per il funzionamento di WPA/TKIP con la scheda client Cisco Aironet serie 350, è necessario disabilitare la convalida dell'handshake WPA poiché al momento esiste un'incompatibilità tra il client CSSC e i driver 350 per quanto riguarda la convalida dell'hash dell'handshake WPA. Questa opzione è disabilitata in **Client > Impostazioni avanzate > Convalida handshake WPA/WPA2**. La convalida dell'handshake disabilitata consente ancora le funzionalità di protezione inerenti a WPA (TKIP per-packet key e Controllo integrità messaggi), ma disabilita l'autenticazione della chiave WPA iniziale.

A		Data Security	
ACC 2.1	kieronkeu (2 soosse detected)	Cala security	H
Ш Э.т	employee least	©© WFA2 ©© \u/DA2	F
	Enterprise (4 accesses detected)		
	00141b5a2bd0 High Signal 00141b5a2bdf High Signal	WPA2 WPA2	
	00141b5a33d0 High Signal 00141b5a33df High Signal	WPA2 WPA2	
îΠ	guest	🗕 Open	
۱II	guest-central	📓 Open	~
CC6	ess (SSID): Enterprise		
] /	Actively search for this access device		
] / En	Actively search for this access device terprise Port Settings:		_

In Riepilogo configurazione di rete fare clic su **Modifica** per configurare le impostazioni EAP / credenziali. Specificare **Turn On** Authentication, Choose **FAST** (Attiva autenticazione) in Protocol (Protocollo), quindi selezionare 'Anonymous' (Anonimo) come Identity (per non usare alcun nome utente nella richiesta EAP iniziale). È possibile utilizzare **Use Username as** Identity come identità EAP esterna, ma molti clienti non desiderano esporre gli ID utente nella richiesta EAP iniziale non crittografata. Specificare **Usa credenziali Single Sign-On** per utilizzare le credenziali di accesso per l'autenticazione di rete. Fare clic su **Configure** (Configura) per impostare i parametri EAP-FAST.

Network Authentication				
Network: Enterprise Network	Lies Cardentiele			
 Turn Off Turn On Use Username as Identity Use 'Anonymous' as Identity Protocol EAP-MD5 EAP-MSCHAPv2 EAP-TLS FAST GTC Configure 	 Use Machine Credentials Use Single Sign on Credentials Request when needed Remember forever Remember for this session Remember for 5 minutes 			
Help	OK Cancel			

Nelle impostazioni FAST è possibile specificare **Validate Server Certificate**, che consente al client di convalidare il certificato del server EAP-FAST (ACS) prima di stabilire una sessione EAP-FAST. In questo modo i dispositivi client sono protetti da connessioni a server EAP-FAST sconosciuti o non autorizzati e dall'invio involontario delle credenziali di autenticazione a una fonte non attendibile. È necessario che nel server ACS sia installato un certificato e nel client sia installato anche il certificato dell'autorità di certificazione radice corrispondente. In questo esempio la convalida del certificato server non è attivata.

Nelle impostazioni FAST è possibile specificare **Allow Fast Session Resumption**, che consente la ripresa di una sessione EAP-FAST in base alle informazioni del tunnel (sessione TLS) anziché in base alla richiesta di una riautenticazione EAP-FAST completa. Se il server e il client EAP-FAST hanno una conoscenza comune delle informazioni sulla sessione TLS negoziate nell'ambito dello scambio di autenticazione iniziale EAP-FAST, è possibile che la sessione venga ripresa.

Nota: sia il server che il client EAP-FAST devono essere configurati per la ripresa delle sessioni EAP-FAST.

In Tunneled Method > EAP-TLS Settings, specificare **Any Method** per consentire il provisioning automatico di EAP-MSCHAPv2 per PAC e EAP-GTC per l'autenticazione. Se si utilizza un database in formato Microsoft, ad esempio Active Directory, e se non supporta alcun client EAP-FAST v1 nella rete, è inoltre possibile specificare l'utilizzo solo di **MSCHAPv2** come metodo di

tunneling.

Nota: Convalida certificato server è abilitato per impostazione predefinita nelle impostazioni EAP-TLS in questa finestra. Poiché nell'esempio non viene utilizzato EAP-TLS come metodo di autenticazione interna, questo campo non è applicabile. Se questo campo è abilitato, il client può convalidare il certificato del server oltre alla convalida del certificato del server all'interno di EAP-TLS.

👁 Configure EAP Method 🛛 🛛
FAST settings: Use Client Certificate Use Smartcard-based Client Certificates Only Validate Server Certificate Allow Fast Session Resumption
Tunneled Method
Any Method
Use Smartcard-based Llient Certificates Unly
✓ Validate Server Certificate
Help OK Cancel

Fare clic su **OK** per salvare le impostazioni EAP-FAST. Poiché il client è configurato per "stabilire automaticamente" nel profilo, avvia automaticamente l'associazione/autenticazione con la rete. Nella scheda Gestisci reti, i campi Rete, Stato e Sicurezza dati indicano lo stato di connessione del client. Nell'esempio viene mostrato che la rete Profile Enterprise è in uso e il dispositivo di accesso alla rete è il SSID Enterprise, che indica Connesso: Autenticato e utilizza la connessione automatica. Il campo Sicurezza dati indica il tipo di crittografia 802.11 utilizzato, che, per questo esempio, è WPA2.

Cisco Secure Services Client			
Client Administration Help			
Create Networks Manage Networks			
Network 🔺	Status	Data Security	
Enterprise Network	Connected: Authenticated		
1 Enterprise	Connected: Authenticated (AutoConnect)	🗃 WPA2	
			Details
Connect	Configure Remove Stat	us	
			.:

Una volta eseguita l'autenticazione del client, scegliere **SSID** in Profilo nella scheda Gestisci reti e fare clic su **Stato** per eseguire una query sui dettagli della connessione. La finestra Dettagli connessione fornisce informazioni sulla periferica client, sullo stato e sulle statistiche della connessione e sul metodo di autenticazione. La scheda Dettagli WiFi fornisce dettagli sullo stato della connessione 802.11, che include RSSI, il canale 802.11 e autenticazione/crittografia.

Connection Status

Connection Details WiFi [Details
Status:	Connected: Authenticated
Duration:	00:00:47
Network Profile:	Enterprise Network
Network Adapter:	Cisco Aironet 802.11a/b/g Wireless Adapter (Microsoft's Packet Scheduler)
Client MAC Address:	00-40-96-A0-36-2F
Access Device:	Enterprise
Access Device MAC Addr	ess: 00-14-1B-5A-33-D0
Transmitted packets:	121
Received packets:	6
Speed:	54.0 Mbps
Authentication Method:	FAST / GTC
Authentication Server:	TME (not verified)
IP Address:	10.10.82.11
Help	Close

X

Connection Status		K
Connection Details WiFi Details		
Connection Details Wiri Details Access Device MAC Address (BSSID): Channel: Signal Strength: Association Method: Encryption:	00-14-1B-5A-33-D0 1 Very High WPA2 Enterprise AES	
Help	Close]

In qualità di amministratore di sistema, l'utente ha diritto all'utilità di diagnostica Cisco Secure Services Client System Report, disponibile con la distribuzione CSSC standard. Questa utilità è disponibile dal menu Start o dalla directory CSSC. Per ottenere i dati, fare clic su **Raccogli dati > Copia negli Appunti > Individua file di report**. In questo modo una finestra Esplora file di Microsoft viene indirizzata alla directory contenente il file del report compresso. All'interno del file compresso, i dati più utili si trovano in log (log_current).

L'utility fornisce lo stato corrente di CSSC, i dettagli dell'interfaccia e del driver, insieme alle informazioni WLAN (SSID rilevato, stato dell'associazione, ecc.). Questa opzione può essere utile, in particolare per diagnosticare i problemi di connettività tra CSSC e la scheda WLAN.

Verifica operazione

Dopo aver configurato il server Cisco Secure ACS, il controller WLAN, il client CSSC e presumibilmente la configurazione corretta e il popolamento del database, la rete WLAN è configurata per l'autenticazione EAP-FAST e la comunicazione sicura con il client. Sono numerosi i punti che possono essere monitorati per controllare lo stato di avanzamento / gli errori per una sessione sicura.

Per verificare la configurazione, tentare di associare un client wireless al controller WLAN con autenticazione EAP-FAST.

 Se CSSC è configurato per la connessione automatica, il client tenta di stabilire la connessione automaticamente. Se non è configurata per la connessione automatica e l'accesso singolo, l'utente deve avviare la connessione WLAN tramite il pulsante di opzione Connetti. In questo modo viene avviato il processo di associazione 802.11 su cui viene eseguita l'autenticazione EAP.Questo è un esempio:

Cisco Secure Services Client		
Client Administration Help		
Create Networks Manage Networks		
Network 🔺	Status	Data Security
Enterprise Network	Disconnected	
Enterprise (hidden)	Not Available (Manual)	B WPA2
		>
	n en carcarcarcarcarcarcarcarcarcarcar en carcarcarcarcarca	Details
Connect Configure	Remove Status	

2. All'utente viene quindi richiesto di fornire il nome utente e la password per l'autenticazione EAP-FAST (dall'autorità EAP-FAST PAC o ACS).Questo è un

	Enter Your Credentials	
	Please enter your credentials for network Enterprise, access akita_pkc	
	osemane. uneusera	
esempio [.]	Send Cancel	
Enter Y	'our Credentials	
	Please enter your credentials for network Enterprise, access akita_pkc	
	Username: tmeuser3	
	Welcome to the Richfield TME PAC Auth	
Dialog e	expires in 10 second(s) Send Cancel	

3. Il client CSSC, tramite il WLC, passa quindi le credenziali utente al server RADIUS (Cisco Secure ACS) per convalidarle. ACS verifica le credenziali utente confrontando i dati e il database configurato (nella configurazione di esempio, il database esterno è Windows Active Directory) e fornisce l'accesso al client wireless ogni volta che le credenziali utente sono valide. Il report Autenticazioni superate sul server ACS indica che il client ha superato l'autenticazione RADIUS/EAP.Questo è un esempio:

Cinca Secreme	Reports and Activity															I
م <u>دالہ</u> جالہ	Select	Select														
Entrance	Reports	Pessed Aut Regular Exp Apply Fil Filtering is	thenticat ression ter C	lans active Gear Filter d.]	Setteeb St.	art Date n/dd/yy	6: Tim yy,hiho	e mm:ss	End Dati mm/dd/	e & Time yyyy,hh:	Re nem:ss 5	ws per Pag D	2		
Configuration Configuration Configuration	KADIUS Accounting VolP Accounting Passed Authentications Faled Attempts	Date +	Lime	Message- Type	User- Name	Group- Nome	Caller- ID	NAS- Part	NAS-IP- Address	Network Access Profile Name	Shared RAC	Downloadable ACL	System- Posture- Token	Application Posture: Taken	Reason	EA
Configuration	Logged-in Users	08/22/2006	16:25:37	Authen OK	test	Default Group	00-40- 96-A0- 36-2F	29	10.10.00.1	(Default)						43
G Contract Uper	Database Replication	08/22/2006	16:09:51	Authen OK	test	Default Group	00-40- 96-A6- 06-F6	29	10.10.80.3	(Default)						42
Reading States of Access	User Password Changes	08/22/2006	16:06:55	Authen OK	test	Default Group	00-40- 96-86- 06-F6	29	10.10.80.3	(Default)						43
States 1	ACS. Service Monitoring	08/22/2006	16:06:39	Authen OK	test	Default Group	00-40- 96-A6- D6-F6	29	10.10.80.3	(Default)						43
Distantion	🔮 Stuck to Help	08/22/2006	16:06:29	Authen OK	test	Default Group	00-40- 96-A6- 06-F6	29	10.10.80.3	(Default)						43

4. Se l'autenticazione RADIUS/EAP ha esito positivo, il client wireless (in questo esempio 00:40:96:ab:36:2f) viene autenticato con il controller AP/WLAN.

Energ Service								Save Carfiguratia	t I Ping I	logist Ref
A. A.	MONITOR WLAP	S CONTROLLER WI	NELESS SECURITY	MANAGEMENT COMM	ANDS HELP					
Wireless	Clients							Rens 1	to 4	of 4
Access Paints ALAPE	Search by NAC a	édress	Search							
802.118 Hadoc 802.118/g Radios	Client MAC Adds	AP Name	WLAN	Туре	Status	Auth Par	t			
Mesh	8810556145154130	AP0854.6948.9594	Usknow	m 882.11b	Probing	No 29	Detail LinkText Disable	Remove 882.11aTSM 902.1	UD/STSN	
Reques	88 x89 /96 x80 36 21	AP0054.6940.8594	Enterpr	ice 882.11g	Associated	Yes 29	Detail LinkText Disable	Remove BELLINTEM 902.1	UD/STSM	
Roque APS	88149796186184165	AP0854.6948.8480	Unknow	m 882.11b	Probing	No 29	Detail LinkText Disable	Remove 882.114TSH 802.1	15/9TSM	
Roove Regue APs Rogue Clients Adhoc Rogues	83140 /961861 dér f6	AP0854.6948.8480	Enterge	ise 882.33g	Associated	No 29	Detail LinkTest Disable	Remove BE2.11aTSM 802.1	LINGTON	
Clients										

Appendice

Oltre alle informazioni di diagnostica e stato, disponibili su Cisco Secure ACS e Cisco WLAN Controller, sono disponibili altri punti per diagnosticare l'autenticazione EAP-FAST. Sebbene la maggior parte dei problemi di autenticazione possa essere diagnosticata senza l'uso di uno sniffer WLAN o il debug degli scambi EAP sul controller WLAN, questo materiale di riferimento è incluso per facilitare la risoluzione dei problemi.

Acquisizione sniffer per Exchange EAP-FAST

Questa acquisizione sniffer 802.11 mostra lo scambio di autenticazione.

Source	Flags	Channel	Signal	Data Rate	Size	Relative Time	Protocol	Summary
00:14:1B:5A:33:D0	*	11	68%	36.0	101	00.033877	802.11 Assoc Rsp	FC=R,SN=2867,FN= 0,Status
00:14:1B:5A:33:D0	+	11	70*	24.0	101	00.036453	802.11 Assoc Rsp	FC=R,SN=2867,FN= 0,Status
00:14:1B:5A:33:D0		11	71%	54.0	90	00.036494	802.1x	FC=.F,SN=2868,FN= 0
Aironet: A0:36:2F		11	54%	1.0	82	00.123205	EAP Response	FC-T,SN- 3,FN- 0
00:14:18:5A:33:D0	1	11	71%	1.0	14	00.123517	802.11 Ack	FC=
00:14:1B:5A:33:D0		11	674	54.0	65	00.165611	802.1x	FC=.F,SN=2870,FN= 0
Aiconet: A0:36:2F		11	55%	1.0	82	00.173920	EAP Response	FC=T,SN= 4,FN= 0
00:14:18:5A:33:D0	8	11	70%	1.0	14	00.174228	802.11 Ack	FC+
00:14:1B:5A:33:D0		11	68%	54.0	66	00.178863	802.1x	FC=.F,SN=2871,FN= 0
Aiconet: A0:36:2F		11	58*	1.0	282	00.200632	EAP Response	FC=T,SN= 5,FN= 0
Aiconet:A0:36:2F		11	584	1.0	282	00.203340	EAP Response	FC=TR,SN= 5,FN= 0
00:14:1B:5A:33:D0	+	11	71%	1.0	14	00.203639	802.11 Ack	FC
00:14:18:5A:33:D0		11	70%	54.0	166	00.207634	802.1x	FC=.F,5N=2872,FN= 0
Aironet:A0:36:2F		11	554	1.0	105	00.216295	EAP Response	FC=T,SN= 6,FN= 0
Aironet: A0:36:2F		11	57%	1.0	105	00.217444	EAP Response	FC-TR,SN= 6,FN= 0
00:14:18:5A:33:D0	1	11	70%	1.0	14	00.217754	802.11 Ack	FC+
00:14:1B:5A:33:D0		11	67%	54.0	99	00.222799	802.1x	FC=.F,SN=2874,FN= 0
Aiconet: A0:36:2F		11	55>	1.0	152	00.254189	EAP Response	FC=T,SN= 7,FN= 0
00:14:18:5A:33:D0	8	11	684	1.0	14	00.254499	802.11 Ack	FC+
00:14:1B:5A:33:D0		11	64%	54.0	147	00.288950	802.1x	FC=.F.R,SN=2875,FN= 0
Aiconet: A0:36:2F		11	553	1.0	232	00.318087	EAP Response	FC=T,SN= 8,FN= 0
00:14:1B:5A:33:D0	¥	11	70%	1.0	14	00.318383	802.11 Ack	FC+
00:14:1B:5A:33:D0		11	68%	54.0	44	00.326833	802.1x	FC=.F,SN=2877,FN= 0
00:14:18:5A:33:D0		11	65%	54.0	44	00.326882	802.1x	FC=.F.R, 5N=2877, FN= 0
00:14:1B:5A:33:D0		11	674	48.0	44	00.326922	802.1x	FC=.F.R,SN=2877,FN= 0
00:14:1B:5A:33:D0		11	678	54.0	157	00.326964	802.1x	FC=.F,SN=2878,FN= 0
Aironet:A0:36:2F		11	57%	1.0	157	00.333742	EAPOL-Key	FC=T,SN= 9,FN= 0
00:14:1B:5A:33:D0	+	11	70%	1.0	14	00.334019	802.11 Ack	FC
00:14:1B:5A:33:D0		11	653	54.0	207	00.340467	802.1x	FC=.F,SN=2879,FN= 0
00:14:1B:5A:33:D0		11	674	54.0	207	00.341130	802.1x	FC=.F.R,SN=2879,FN= 0
Aironet: A0:36:2F		11	57%	1.0	135	00.342542	EAPOL-Key	FC-T,SN- 10,FN- 0

Questo pacchetto mostra la risposta EAP-FAST EAP iniziale.

Nota: come configurato nel client CSSC, nella risposta EAP iniziale viene utilizzato anonimo come identità EAP esterna.

Pasket: 12 🕅 🖘 🕽	
- Frame Control Flags:	+0000001 [1]
-9	0 Non-strict order
-9	.0WIF Not Enabled
-9	No More Data
-0	0 Fower Management = active mode
-0	0 This is not a Re-Transmission
-0	
-9	0. Not an Exit from the Distribution System
-9	1 To the Distribution System
-@ Buration:	314 Microseconds (2-3)
BSSID:	00:14:1B:5A:33:D0 [4-9]
- Source :	00:40:96:A0:36:27 Airconet:A0:36:2F [10=15]
- Bestination:	00:14:18:5A:33:D0 [16-21]
-@ Seg. Number:	3 [22-23 Hask 0x7770]
- @ Frag. Number:	0 [22 Hash 0x07]
- T 802.2 Logical Link Conta	ol (LLC) Keader
-@ Best. SRP:	0%AA SWAP (24)
-@ Source SAP:	OTAA SWAF [25]
-@ Connaad:	0x03 Unnumbered Information [26]
-@ Vendor ID:	0x000000 [27-29]
- @ Protocol Type:	0x888# #02.ix Authentication [30-31]
# ##2.1x Authentication	
- Protocol Version:	1 [32]
-@ Packet Type:	0 IAP - Fackat [33]
- @ Body Length:	14 [34-35]
B-T Extensible Authentica	tion Protocol
- G Code:	2 Response [36]
- G Identifier:	1 [37]
-(3 Length:	14 [38-39]
- (J Type:	1 Zolarstzty (40)
- (j) Type-Bata:	anonymous [41-49]

Debug sul controller WLAN

Questi comandi di debug possono essere usati sul controller WLAN per monitorare lo stato dello scambio di autenticazione:

- debug aaa events enable
- abilitazione dettagli debug aaa

debug dot1x events enable

debug dot1x stati enable

Questo è un esempio di come avviare una transazione di autenticazione tra il client CSSC e l'ACS monitorato sul controller WLAN con i debug:

```
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Processing RSN IE type 48,
   length 20 for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received RSN IE with
   0 PMKIDs from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f dot1x -
  moving mobile 00:40:96:a0:36:2f into Connecting state
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAP-
  Request/Identity to mobile 00:40:96:a0:36:2f (EAP Id 1)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received Identity Response
   (count=1) from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f EAP State update from
  Connecting to Authenticating for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f dot1x - moving mobile
  00:40:96:a0:36:2f into Authenticating state
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Entering Backend Auth
  Response state for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: AuthenticationRequest: 0x138dd764
Thu Aug 24 18:20:54 2006:
                           Callback.....0x10372764
                              protocolType...0x00040001
Thu Aug 24 18:20:54 2006:
Thu Aug 24 18:20:54 2006:proxyState....00:40:96:A0:36:2F-11:00Thu Aug 24 18:20:54 2006:Packet contains 15 AVPs (not shown)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Successful transmission of
  Authentication Packet (id 84) to 10.1.1.12:1812, proxy state0
Thu Aug 24 18:20:54 2006: ****Enter processIncomingMessages: response code=11
Thu Aug 24 18:20:54 2006: ****Enter processRadiusResponse: response code=11
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Access-Challenge received from
  RADIUS server 10.1.1.12 for mobile 00:40:96:a0:36:2f rec7
Thu Aug 24 18:20:54 2006: AuthorizationResponse: 0x11c8a394
Thu Aug 24 18:20:54 2006: structureSize..147
                              resultCode....255
protocolUsed...0x00000001
Thu Aug 24 18:20:54 2006:
Thu Aug 24 18:20:54 2006:
                           proxyState....00:40:96:A0:36:2F-11:00
Thu Aug 24 18:20:54 2006:
Thu Aug 24 18:20:54 2006:
                                Packet contains 4 AVPs (not shown)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Processing Access-Challenge
  for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Entering Backend Auth Req state
  (id=249) for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f WARNING:
   updated EAP-Identifer 1 ===> 249 for STA 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAP Request from
  AAA to mobile 00:40:96:a0:36:2f (EAP Id 249)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAP Response from
  mobile 00:40:96:a0:36:2f (EAP Id 249, EAP Type 3)
```

In questo modo lo scambio EAP dal debug del controller è stato completato (con autenticazione WPA2):

Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Processing Access-Accept for mobile 00:40:96:a0:36:2f Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Applying new AAA override for station 00:40:96:a0:36:2f Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Override values for station

00:40:96:a0:36:2f source: 4, valid bits: 0x0 qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1 dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, r1' Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Unable to apply override policy for station 00:40:96:a0:36:2f - VapAllowRadiusOverride E Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Creating a new PMK Cache Entry for station 00:40:96:a0:36:2f (RSN 2) Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Adding BSSID 00:14:1b:5a:33:d0 to PMKID cache for station 00:40:96:a0:36:2f Thu Aug 24 18:20:54 2006: New PMKID: (16) Thu Aug 24 18:20:54 2006: [0000] a6 c0 02 95 66 e8 ed 9b 1c 65 9b 72 1f 3f 5f 5b Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAP-Success to mobile 00:40:96:a0:36:2f (EAP Id 0) Thu Aug 24 18:20:54 2006: Including PMKID in M1 (16) Thu Aug 24 18:20:54 2006: [0000] a6 c0 02 95 66 e8 ed 9b 1c 65 9b 72 1f 3f 5f 5b Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAPOL-Key Message to mobile 00:40:96:a0:36:2f state INITPMK (message 1), repl0 Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Entering Backend Auth Success state (id=0) for mobile 00:40:96:a0:36:2f Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received Auth Success while in Authenticating state for mobile 00:40:96:a0:36:2f Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f dot1x moving mobile 00:40:96:a0:36:2f into Authenticated state Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAPOL-Key from mobile 00:40:96:a0:36:2f Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Invalid EAPOL version (1) in EAPOL-key message from mobile 00:40:96:a0:36:2f Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAPOL-key in PKT_START state (message 2) from mobile 00:40:96:a0:36:2f Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Stopping retransmission timer for mobile 00:40:96:a0:36:2f Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAPOL-Key Message to mobile 00:40:96:a0:36:2f state PTKINITNEGOTIATING (messal Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAPOL-Key from mobile 00:40:96:a0:36:2f Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Invalid EAPOL version (1) in EAPOL-key message from mobile 00:40:96:a0:36:2f Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAPOL-key in PTKINITNEGOTIATING state (message 4) from mobile 00:40:96:a0:36:2f Thu Aug 24 18:20:54 2006: AccountingMessage Accounting Interim: 0x138dd764 Thu Aug 24 18:20:54 2006: Packet contains 20 AVPs: Thu Aug 24 18:20:54 2006: AVP[01] User-Name.....enterprise (10 bytes) Thu Aug 24 18:20:54 2006: AVP[02] Nas-Port.....0x0000001d (29) (4 bytes) Thu Aug 24 18:20:54 2006: AVP[03] Nas-Ip-Address......0x0a0a5003 (168448003) (4 bytes) Thu Aug 24 18:20:54 2006: AVP[04] Class.....CACS:0/28b5/a0a5003/29 (22 bytes) Thu Aug 24 18:20:54 2006: AVP[05] NAS-Identifier.....ws-3750 (7 bytes) Thu Aug 24 18:20:54 2006: AVP[06] Airespace / WLAN-Identifier.....0x00000001 (1) (4 bytes) Thu Aug 24 18:20:54 2006: AVP[07] 96:a0:36:2f/14 (29 bytes) Thu Aug 24 18:20:54 2006: AVP[08] Thu Aug 24 18:20:54 2006: AVP[09] Thu Aug 24 18:20:54 2006: AVP[10]

Tunnel-Medium-Type.....0x00000006 (6) (4 bytes) Thu Aug 24 18:20:54 2006: AVP[11] Tunnel-Group-Id.....0x3832 (14386) (2 bytes) Thu Aug 24 18:20:54 2006: AVP[12] Acct-Status-Type.....0x00000003 (3) (4 bytes) Thu Aug 24 18:20:54 2006: AVP[13] Acct-Input-Octets......0x000b99a6 (760230) (4 bytes) Thu Aug 24 18:20:54 2006: AVP[14] Acct-Output-Octets......0x00043a27 (277031) (4 bytes) Thu Aug 24 18:20:54 2006: AVP[15] Acct-Input-Packets......0x0000444b (17483) (4 bytes) Thu Aug 24 18:20:54 2006: AVP[16] Acct-Output-Packets......0x0000099b (2459) (4 bytes) Thu Aug 24 18:20:54 2006: AVP[17] Thu Aug 24 18:20:54 2006: AVP[18] Acct-Delay-Time......0x00000000 (0) (4 bytes) Thu Aug 24 18:20:54 2006: AVP[19] Calling-Station-Id......10.10.82.11 (11 bytes) Thu Aug 24 18:20:54 2006: AVP[20] Called-Station-Id.....10.10.80.3 (10 bytes) Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Stopping retransmission timer for mobile 00:40:96:a0:36:2f Thu Aug 24 18:20:57 2006: User admin authenticated

Informazioni correlate

- Guida all'installazione di Cisco Secure ACS per Windows Server
- Guida alla configurazione di Cisco Secure ACS 4.1
- Esempio di limitazione dell'accesso WLAN in base al SSID con WLC e Cisco Secure ACS
- EAP-TLS in Unified Wireless Network con ACS 4.0 e Windows 2003
- Esempio di assegnazione dinamica di VLAN con il server RADIUS e il controller LAN wireless
- Documentazione e supporto tecnico Cisco Systems