Possibilità di associazione durante l'aggiornamento del firmware del punto di accesso

Sommario

Introduzione

Questo documento descrive il motivo per cui il client non può associarsi a un Access Point (AP) nelle seguenti condizioni:

- Esegue il protocollo LEAP (Lightweight Extensible Authentication Protocol)/ACS (asynchronous communications server).
- Il firmware dell'access point è aggiornato alla versione 11.06 o successive.
- Il firmware del client è aggiornato alla versione 4.25.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

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

- AP340 versione firmware 11.06 e PC340 versione firmware 4.25.5.
- AP AIR-AP342E2R e adattatore client AIR-PCM342.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico

ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Problema 1

Le versioni 11.06 e successive del firmware dell'access point sono conformi agli standard IEEE 802.1X Draft 10. Lo standard Draft 8 è stato utilizzato prima di questa release. La versione 4.25 del firmware sui client è conforme alla bozza 10. Su un access point con firmware 11.06, è possibile utilizzare entrambe le bozze. Se si desidera associare i client che eseguono il firmware 4.23 e versioni precedenti, utilizzare la bozza 8. Un client 4.25 non funziona con un access point 11.06 che utilizza la configurazione Draft 8 e un client 4.25 non funziona con un access point 11.05.

Versione firmware AP	Versione firmware client	Bozza IEEE 802.1X
11.06 (e successive)	4.25	10
	4.23 o precedente	8
11.03--11.05	4.25 (non funziona con 11.05)	L'access point richiede 8, ma il client non funziona con 8
	4.23 o precedente	8

Soluzione 1

Per risolvere il problema, è possibile procedere in due modi:

1. Usare Draft 10 (11.06) sull'access point e aggiornare il firmware delle schede client alla versione 4.25.
2. Usare la bozza 8 sull'access point e usare l'access point con firmware precedente sui client.

Nella tabella sono riportati gli standard bozza IEEE 802.1X a cui sono conformi le diverse versioni del firmware dell'adattatore client (e del firmware di Workgroup Bridge).

Firmware client Version	Bozza 8	Bozza 10
4.13	x	-
4.16	x	-
4.23	x	-
4.25 o successiva	-	x
WGB340/350 8,58	x	-

WGB340/350 8,61	-	x

Problema 2

Viene utilizzata l'autenticazione MAC con il server RADIUS. Alcuni access point Aironet 1231G (AP da Cisco IOS® versione 12.3(7)JA1 a 12.3(7)JA3,) hanno problemi con l'autenticazione dell'utente.

Questo è un problema comune se si esegue l'aggiornamento da una versione più recente di Cisco IOS alla versione 12.3(7)JA3.

Soluzione 2

Per risolvere il problema, occorre innanzitutto verificare la configurazione. Attenersi alla seguente procedura:

1. Rimuovere la chiave di crittografia in SECURITY > Encryption Manager.
2. Fare clic su **Nessuno**, quindi su Applica.
3. Andare a Gestione SSID, evidenziare il **nome_SSID** SSID, quindi scegliere **<NESSUNA AGGIUNTA>**.
4. Dal menu Apri autenticazione, scorrere verso il basso e fare clic su **Applica**.Una volta applicate queste modifiche, è possibile eseguire il test con l'adattatore client.Se il problema persiste, anche senza le impostazioni di crittografia e autenticazione, è preferibile ripristinare l'access point ai valori predefiniti e riconfigurarlo da zero.
5. Completare questa procedura per ripristinare l'access point ai valori predefiniti:Scegliere **Software di sistema > Configurazione di sistema**.Fare clic su **Ripristina valori predefiniti** (eccetto IP).Una volta riavviato, è possibile riconfigurarlo e provare con l'adattatore client.
6. Verificare l'impostazione Autenticazione MAC in Protezione avanzata e impostarla su Solo server. Attenersi alla seguente procedura:Scegliere **Sicurezza > Sicurezza avanzata > Autenticazione MAC**.Fare clic su Solo **server**.Fare clic sull'impostazione **Salva**.

Informazioni correlate

- Suggerimenti tecnici per le reti LAN wireless
- Documentazione e supporto tecnico – Cisco Systems