

Konfigurieren des Management Frame Protection (MFP) auf einem Wireless Access Point

Ziel

Management Frame Protection (MFP) ist eine Wireless-Funktion, die die Sicherheit der Management-Frames erhöht. Der Wireless-Standard ist IEEE 802.11w-2009 oder Protected Management Frames (PMF), der die Vertraulichkeit der Daten der Management-Frames sicherstellen und die Wireless-Konnektivität schützen soll. Diese Funktion funktioniert nur, wenn sowohl der Access Point als auch der Client MFP aktiviert haben.

Einige Wireless-Clients können nur mit MFP-fähigen Infrastrukturgeräten kommunizieren. MFP fügt jeder Anfrage oder jedem SSID-Beacon eine Reihe von Informationselementen hinzu. Einige Wireless-Clients wie Personal Digital Assistants (PDAs), Smartphones, Barcode-Scanner usw. verfügen über einen begrenzten Arbeitsspeicher und eine begrenzte CPU, sodass Sie diese Anfragen oder Beacons nicht verarbeiten können. Aus diesem Grund wird der Service Set Identifier (SSID) nicht vollständig angezeigt, oder die Verbindung mit diesen Infrastrukturgeräten kann aufgrund von Diskrepanzen zwischen den SSID-Funktionen nicht hergestellt werden. Dieses Problem betrifft nicht nur den MFP. Dies gilt auch für alle SSIDs mit mehreren Informationselementen (IEs). Es wird immer empfohlen, MFP-fähige SSIDs in der Umgebung mit allen verfügbaren Clienttypen zu testen, bevor Sie sie in Echtzeit bereitstellen.

Dieser Artikel enthält Anweisungen zur Konfiguration von MFP auf Ihrem Wireless Access Point (WAP).

Hinweis: Diese Funktion wird möglicherweise von Ihrem Wireless-Client oder -Betriebssystem nicht unterstützt. Weitere Informationen erhalten Sie von Ihrem Hersteller des Wireless-Geräts oder -Betriebssystems.

Anwendbare Geräte

WAP100-Serie - WAP150

WAP300-Serie - WAP361, WAP371

WAP500-Serie

Softwareversion

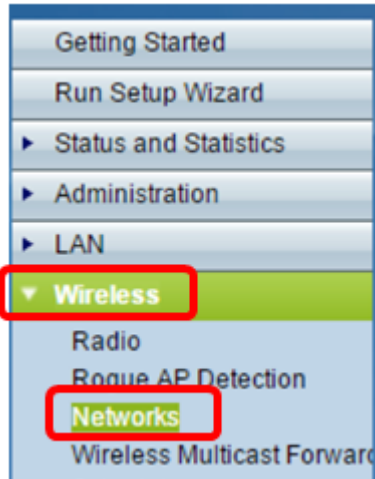
1.2.1.3 - WAP371, WAP551, WAP561

1.0.0.16 - WAP150, WAP361, WAP571, WAP571E

Konfigurieren von MFP auf einem WAP

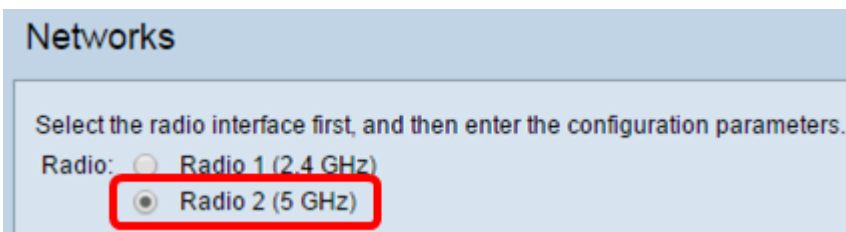
Wichtig: Vergewissern Sie sich, dass Ihr Wireless-Netzwerk konfiguriert wurde, bevor Sie mit den Konfigurationsschritten fortfahren.

Schritt 1: Melden Sie sich beim webbasierten Access Point-Dienstprogramm an, und wählen Sie dann **Wireless > Networks** aus.



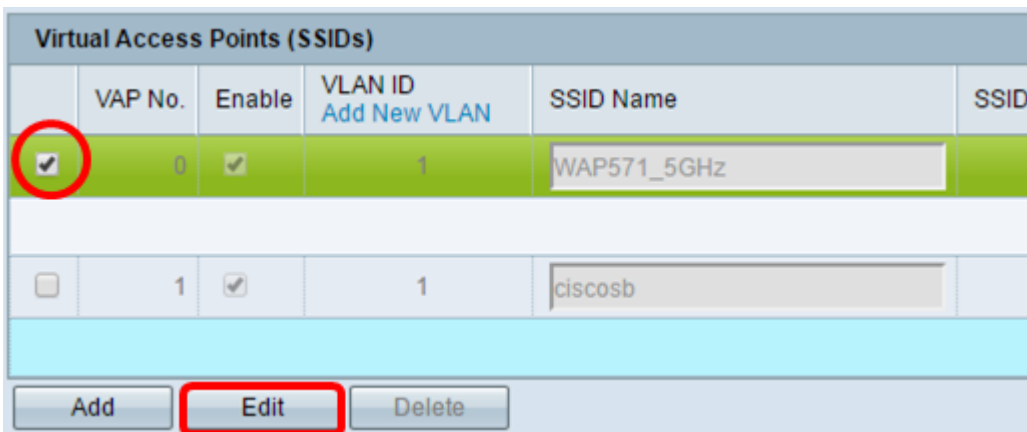
Schritt 2: Wählen Sie im Bereich Radio (Funkübertragung) der Seite Networks (Netzwerke) ein Optionsfeld aus, in dem Ihre Service Set Identifier (SSID) konfiguriert ist. Radios können je nach dem vorhandenen WAP-Modell variieren. In diesem Beispiel wird Radio 2 (5 GHz) ausgewählt.

Hinweis: Wenn Sie einen WAP551 haben, fahren Sie mit [Schritt 3 fort](#). WAP551 ist ein Single-Band-Access Point.



[Schritt 3:](#) Aktivieren Sie unter den virtuellen Zugangspunkten (SSIDs) das Kontrollkästchen der SSID, die Sie konfigurieren möchten, und klicken Sie dann auf **Bearbeiten**.

Hinweis: In diesem Szenario wird WAP571 verwendet.



Schritt 4: Klicken Sie auf **Details anzeigen**.

SSID Name	SSID Broadcast	Security	MAC Filter
WAP571_5GHz	<input checked="" type="checkbox"/>	WPA Personal ▼	Disabled ▼
Show Details			
ciscosb	<input checked="" type="checkbox"/>	WPA Personal ▼	Disabled ▼
Show Details			

Schritt 5: Aktivieren Sie im Bereich WPA-Versionen das Kontrollkästchen **WPA2-AES**.

Security	MAC Filter	Channel Isolation
WPA Personal ▼	Disabled ▼	<input checked="" type="checkbox"/>
Hidden Details		
WPA Versions:	<input type="checkbox"/> WPA-TKIP	<input checked="" type="checkbox"/> WPA2-AES
Key:	<input type="text" value="....."/> (Range: 8 - 63 Characters) <input type="checkbox"/> Show Key as Clear Text	
Key Strength Meter:	<input type="text" value=" "/> Weak	
Broadcast Key Refresh Rate	<input type="text" value="86400"/> Sec (Range: 0 - 86400, 0 = Disabl	
MFP:	<input type="checkbox"/> Not Required <input checked="" type="checkbox"/> Capable <input type="checkbox"/> Required	

Schritt 6: (Optional) Wenn das Kontrollkästchen WPA-TKIP im Bereich WPA-Versionen aktiviert ist, deaktivieren Sie das Kontrollkästchen, um die MFP-Optionen anzuzeigen. Die WPA-TKIP-Sicherheit unterstützt die MFP-Funktion nicht.

Security	MAC Filter	Channel Isolation	Be
WPA Personal ▼	Disabled ▼	<input checked="" type="checkbox"/>	
Hidden Details			
WPA Versions:	<input checked="" type="checkbox"/> WPA-TKIP	<input checked="" type="checkbox"/> WPA2-AES	
Key:	<input type="text" value="....."/> (Range: 8 - 63 Characters) <input type="checkbox"/> Show Key as Clear Text		
Key Strength Meter:	<input type="text" value=" "/> Weak		
Broadcast Key Refresh Rate	<input type="text" value="86400"/> Sec (Range: 0 - 86400, 0 = Disable,		

Schritt 7: Aktivieren Sie im Bereich MFP das Kontrollkästchen **Required MFP**.

Key Strength Meter:	<input type="text" value=" "/> Weak
Broadcast Key Refresh Rate	<input type="text" value="86400"/> Sec (Range: 0 - 86400, 0 = Disable,
MFP:	<input type="checkbox"/> Not Required <input checked="" type="checkbox"/> Capable <input checked="" type="checkbox"/> Required

Folgende Optionen stehen zur Verfügung:

Not Required (Nicht erforderlich) - Deaktiviert die Client-Unterstützung für MFP.

Capable (MFP) - Ermöglicht MFP-fähigen und Clients, die MFP nicht unterstützen, dem Netzwerk beizutreten. Dies ist die Standard-MFP-Einstellung für den WAP.

Erforderlich - Kunden können nur eine Verbindung herstellen, wenn ein MFP ausgehandelt wird. Wenn die Geräte MFP nicht unterstützen, sind sie nicht berechtigt, dem Netzwerk beizutreten.

Schritt 8: Klicken Sie auf **Speichern**.

Select the radio interface first, and then enter the configuration parameters.

Radio: Radio 1 (5 GHz)
 Radio 2 (2.4 GHz)

Virtual Access Points (SSIDs)					
	VAP No.	Enable	VLAN ID Add New VLAN	SSID Name	SSID
<input checked="" type="checkbox"/>	0	<input checked="" type="checkbox"/>	1 ▼	WAP571_5GHz	
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	1	ciscosb	

Schritt 9: Wenn das Fenster Pop-up bestätigen angezeigt wird, klicken Sie auf **OK**.

Confirm

Your wireless settings are about to be updated. You may be disconnected.

Sie sollten jetzt MFP für Ihren Access Point konfiguriert haben.

Sehen Sie sich ein Video zu diesem Artikel an..

[Klicken Sie hier, um weitere Tech Talks von Cisco anzuzeigen.](#)