



暗号化トンネル導入ガイド

[はじめに](#) 2

[前提条件](#) 2

[製品や機能の概要](#) 2

[暗号化モビリティ トンネルの設定](#) 3

はじめに

このドキュメントでは、8.7 モビリティ暗号化トンネルとその導入についての一般的なガイドラインを示します。このドキュメントの目的は以下のとおりです。

- 8.7 モビリティ暗号化トンネル機能の概要を提供する
- サポートされている主要機能のハイライト
- 8.7 モビリティ暗号化トンネル機能の導入と管理の詳細を提供する

前提条件

8.5MR1 または 8.7 コードにアップグレードするには、ワイヤレス LAN コントローラに AireOS 8.0 以降のリリースを用意する必要があります。

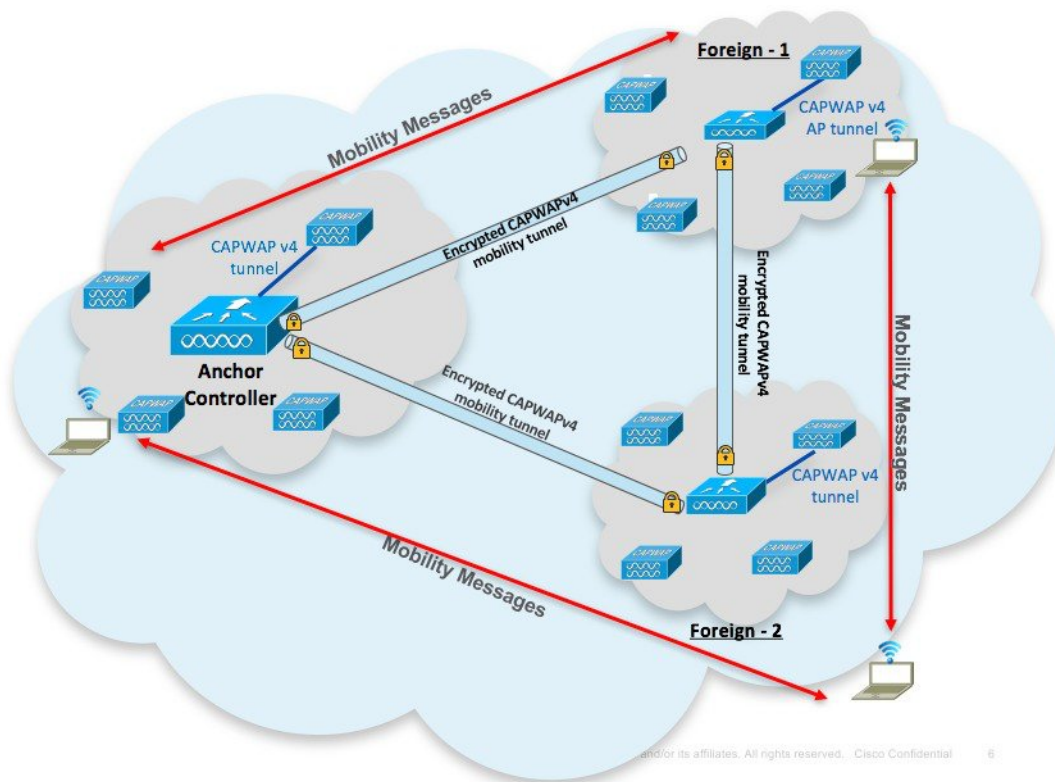


(注) この機能は、8.5MR1 と 8.7 およびそれ以降のリリースでのみ機能し、3504、5520、8540 のコントローラでサポートされます。

製品や機能の概要

このドキュメントでは、アンカーとフォーリン WLC 間のモビリティトンネルでエンドツーエンドの暗号化をサポートするシステムの概要を説明します。さらに、アンカーとフォーリン WLC 間でモビリティトンネルのエンドツーエンドの暗号化をサポートするための WLC 側の基本的前提についても説明します。

以下の図に、アンカーとフォーリン WLC 間のモビリティトンネルのエンドツーエンドの暗号化のアーキテクチャを示します。このアーキテクチャで WLC は、WLC 間に DTLS 暗号化を使用する CAPWAP ベースのモビリティトンネルを介して接続されています。クライアントデータは、AP から WLC、およびフォーリンとアンカー WLC 間で安全な DTLS 暗号化 CAPWAP トンネルを介して渡されます。つまり、DTLS 暗号化を使用する CAPWAP ベースのモビリティトンネルを介して渡されます。このように、クライアントデータは、クライアントネットワークからアンカー WLC までのデータパス全体で暗号化トンネルを介して渡されるため、中間者によるスヌーピングが行われる余地がありません。



- リリース 8.7 では、アンカーとフォーリン コントローラ間のトンネルがエンドツーエンドで暗号化されている
- 暗号化トンネルでは CAPWAP v4 と DTLS 暗号化が使用される
- 新旧のモビリティ アーキテクチャがサポートされる
- Client SSO がサポートされる
- 3504、5520、8540 コントローラでサポートされている

暗号化モビリティ トンネルの設定

リリース 8.7 でエンド ツー エンドの暗号化モビリティ トンネルを設定するには、以下の手順に従います。

手順

ステップ 1 モビリティ グループのやり取りに参加する必要があるすべてのコントローラを設定します。すべてのコントローラに、相互の情報を設定する必要があります。

Local Mobility Group	miadler					
MAC Address	IP Address (IPv4/IPv6)	Group Name	Multicast IP	Status	Hash Key	
fc:5b:39:aa:62:b5	10.70.0.18	miadler	0.0.0.0	Up	none	
00:24:97:cc:71:e0	10.50.10.24	miadler	0.0.0.0	Up	none	
00:b0:e1:f2:2a:00	10.70.0.19	miadler	0.0.0.0	Up	none	
00:b0:e1:f2:39:00	10.70.0.17	miadler	0.0.0.0	Up	none	
fc:5b:39:aa:62:b5	2001::10:70:18	miadler	::	Up	none	

```
(Cisco Controller) >config mobility group member add ?
```

```
<IP addr>      Member switch IP address
```

ステップ2 コントローラごとに、Mobility Encryption を有効にします。

Mobility Encryption を有効にすると、コントローラが再起動します。

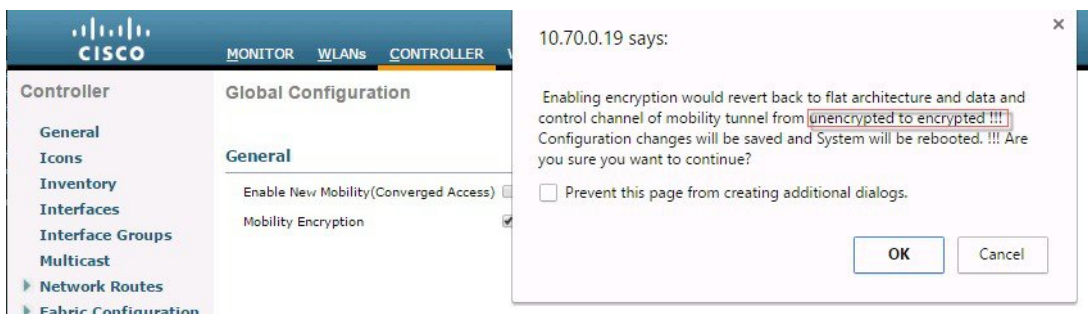


```
(Cisco Controller) >config mobility encryption ?
```

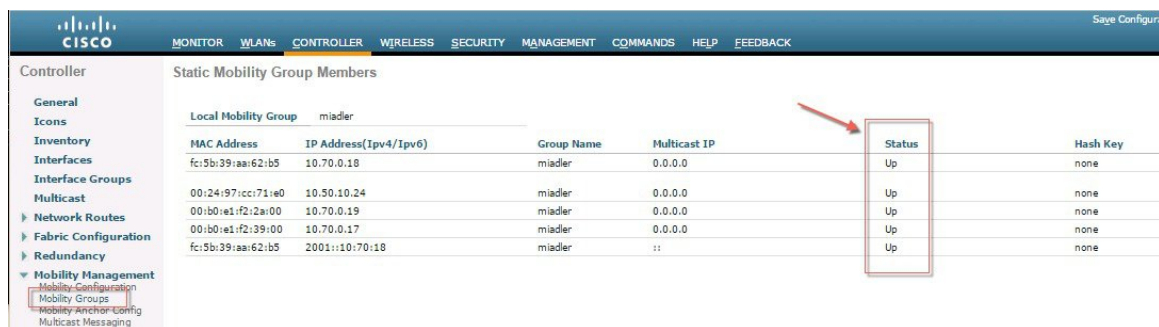
```
enable          Enables the encryption feature.
```

```
disable         Disables the encryption feature.
```

ステップ3 再起動の前にコントローラは次のメッセージを表示するため、[OK] をクリックして変更を適用します。



ステップ4 暗号化モビリティトンネルが設定されたコントローラが起動すると、[Status] に Up と表示されます。



Local Mobility Group	MAC Address	IP Address(Ipv4/Ipv6)	Group Name	Multicast IP	Status	Hash Key
miadler	fc:5b:39:aa:62:b5	10.70.0.18	miadler	0.0.0.0	Up	none
	00:24:97:cc:71:e0	10.50.10.24	miadler	0.0.0.0	Up	none
	00:b0:e1:f2:2a:00	10.70.0.19	miadler	0.0.0.0	Up	none
	00:b0:e1:f2:39:00	10.70.0.17	miadler	0.0.0.0	Up	none
	fc:5b:39:aa:62:b5	2001::10:70:18	miadler	::	Up	none

図 1:

```
(Cisco Controller) >show mobility summary
```

Mobility Protocol Port..... 16666
 Default Mobility Domain..... miadler
 Multicast Mode..... Disabled
 DTLS Mode..... Enabled
 Mobility Domain ID for 802.11r..... 0x2b12
 Mobility Keepalive Interval..... 10
 Mobility Keepalive Count..... 3
 Mobility Group Members Configured..... 4
 Mobility Control Message DSCP Value..... 0

MAC Address	IP Address	Status	Group Name	Multicast IP
00:24:97:cc:71:e0	10.50.10.24	Control and Data Path Down	miadler	0.0.0.0
00:b0:e1:f2:2a:00	10.70.0.19	Up	miadler	0.0.0.0
00:b0:e1:f2:39:00	10.70.0.17	Up	miadler	0.0.0.0
fc:5b:39:aa:62:b5	10.70.0.18	Up	miadler	0.0.0.0

ステップ5 Mobility Encryption が有効になり、トンネルリンクのステータスが Up になると、暗号化された接続が確立されていることを確認するためにさらにもう 1 つチェックを実行できます。暗号化トンネル経由で、あるコントローラから別のコントローラの IP アドレスに MPING を実行し、MPING が成功することを確認します。

```
(Cisco Controller) >show mobility summary
```

DTLS Mode..... Enabled
 Mobility Domain ID for 802.11r..... 0x2b12
 Mobility Keepalive Interval..... 10
 Mobility Keepalive Count..... 3
 Mobility Group Members Configured..... 4
 Mobility Control Message DSCP Value..... 0

MAC Address	IP Address	Status	Group Name	Multicast IP
00:24:97:cc:71:e0	10.50.10.24	Control and Data Path Down	miadler	0.0.0.0
00:b0:e1:f2:2a:00	10.70.0.19	Up	miadler	0.0.0.0
00:b0:e1:f2:39:00	10.70.0.17	Up	miadler	0.0.0.0
fc:5b:39:aa:62:b5	10.70.0.18	Up	miadler	0.0.0.0

```
(Cisco Controller) >mping 10.70.0.17
```

Send count=3, Receive count=3 from 10.70.0.17

```
(Cisco Controller) >
```

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

©2008 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。

本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R)

この資料の記載内容は2008年10月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>