



ワイヤレス ゲスト アクセスの設定

- [機能情報の確認, 1 ページ](#)
- [ゲスト アクセスの前提条件, 1 ページ](#)
- [ゲスト アクセスの制約事項, 2 ページ](#)
- [ワイヤレス ゲスト アクセスについて, 2 ページ](#)
- [高速安全ローミング, 2 ページ](#)
- [ゲスト アクセスを設定する方法, 3 ページ](#)
- [ゲスト アクセスの設定例, 17 ページ](#)
- [ゲスト アクセスに関する追加情報, 23 ページ](#)
- [ゲスト アクセスの機能履歴と情報, 24 ページ](#)

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの [Bug Search Tool](#) およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコソフトウェア イメージのサポートに関する情報を検索するには、[Cisco Feature Navigator](#) を使用します。[Cisco Feature Navigator](#) には、<http://www.cisco.com/go/cfn> からアクセスします。[Cisco.com](#) のアカウントは必要ありません。

ゲスト アクセスの前提条件

- すべてのモビリティ ピアは、階層モビリティ アーキテクチャに対して設定されている必要があります。

- WLAN上のゲストコントローラ モビリティ アンカーの設定は、モビリティ エージェントおよびゲスト コントローラ上である必要があります。
 - ゲスト アクセスは、3 ボックス ソリューションまたは2 ボックス ソリューションが可能です。モビリティ トンネルのリンク ステータスは、以下の間で適用される必要があります。
 - モビリティ エージェント、モビリティ コントローラおよびゲスト コントローラ。
- または
- モビリティ エージェント/モビリティ コントローラおよびゲスト コントローラ。

ゲスト アクセスの制約事項

ゲストコントローラの機能は、Catalyst 3850 スイッチでサポートされていませんが、Catalyst 3850 はモビリティ エージェントとして機能できます。

ワイヤレス ゲスト アクセスについて

理想としては、ワイヤレスゲストネットワークの実装で、企業の既存のワイヤレスおよび有線インフラストラクチャを最大限活用して、物理オーバーレイ ネットワークを構築する際のコストや複雑さを回避します。この場合は、次の要素と機能の追加が必要になります。

- 専用のゲスト WLAN/SSID：ゲストアクセスを必要とするあらゆる場所で、キャンパス ワイヤレス ネットワークを介して実装されます。ゲスト WLAN は、モビリティ アンカー（ゲスト コントローラ）が設定された WLAN で識別されます。
- ゲストトラフィックのセグメンテーション：ゲストの移動場所を制限するために、キャンパス ネットワーク上のレイヤ2 またはレイヤ3 での実装テクニックを必要とします。
- アクセス コントロール：キャンパス ネットワーク内に組み込まれたアクセス コントロール機能の使用、または企業ネットワークからインターネットへのゲストアクセスを制御する外部プラットフォームの実装を伴います。
- ゲストユーザ資格情報の管理：スポンサーまたはLobby管理者がゲストの代わりに仮の資格情報を作成できるプロセス。この機能は、アクセス コントロールプラットフォーム内に常駐している場合と、AAAなどの管理システムのコンポーネントになっている場合があります。

高速安全ローミング

高速セキュア ローミングは、Cisco Centralized Key Management (CCKM)、802.11r および 802.11i クライアントの Pairwise Master Key (PMK) 情報をキャッシュすることで実現できます。Cisco

Centralized Key Management (CCKM) はローミングの向上に役立ちます。クライアントのみがローミングプロセスを開始できますが、以下のような要因に影響されます。

- AP 間のオーバーラップ
- AP 間の距離
- チャンネル、シグナル強度、および AP 上のロード
- データ レートと出力電力

高速ローミング クライアント (802.11i、[CCKM]) が新しいデバイスにローミングする場合は常に、クライアントは高速ローミング後にモビリティ「ハンドオフ」手順を実行します。また、モビリティ「ハンドオフ」手順後に学習した AAA 属性が再適用されます。

クライアントが 802.11i WPA2、CCKM、802.11r を使用している場合、高速セキュア ローミングの要件をすべて満たすために、ローミング中の完全な L2 認証を避ける必要があります。完全な L2 認証を避けるため、認証およびローミング クライアントのキーの継承に PMK キャッシュ (802.11i、CCKM、および 802.11r) が使用されます。これには、モビリティ グループ内のモビリティアンカー (MA) およびモビリティ コントローラ (MC) が同じ PMK キャッシュ値を持つことが必要です。

セッションタイムアウトは、PMK キャッシュの有効期限を定義します。クライアントが再認証に失敗した場合、または CLI から手動で削除された場合、PMK キャッシュも削除される場合があります。オリジナルのコントローラまたはスイッチの削除は、同じモビリティ グループ内の他のコントローラまたはスイッチにも影響します。

ゲストアクセスを設定する方法

ロビー管理者アカウントの作成

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device # configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	user-name user-name 例： Device (config)# user-name lobby	ユーザ アカウントを作成します。

	コマンドまたはアクション	目的
ステップ 3	type lobby-admin 例： Device (config-user-name)# type lobby-admin	ロビー管理者としてアカウントタイプを指定します。
ステップ 4	password 0 password 例： Device (config-user-name)# password 0 lobby	ロビー管理者アカウントのパスワードを作成します。
ステップ 5	end 例： Device (config-user-name)# end	特権 EXEC モードに戻ります。
ステップ 6	show running-config section user-name または show running-config section 設定したロビー管理者のユーザ名 例： Device # show running-config section lobby	設定の詳細を表示します。

ゲストユーザアカウントの設定

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device # configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 2	user-name user-name 例： Device (config)# user-name guest	Lobby Ambassador アカウントのユーザ名を作成します。
ステップ 3	password unencrypted/hidden-password password 例： Device (config-user-name)# password 0 guest	ユーザのパスワードを指定します。

	コマンドまたはアクション	目的
ステップ 4	type network-user description description guest-user lifetime year 0-1 month 0-11 day 0-30 hour 0-23 minute 0-59 second 0-59 例 : Device (config-user-name)# type network-user description guest guest-user lifetime year 1 month 10 day 3 hour 1 minute 5 second 30	ユーザのタイプを指定します。
ステップ 5	end 例 : Device (config-user-name)# end	特権 EXEC モードに戻ります。
ステップ 6	show aaa local netuser all 例 : Device # show aaa local netuser all	設定の詳細を表示します。有効期間後に、ゲストタイプとユーザ名は削除され、ゲストユーザ名と関連付けられるクライアントは認証解除されます。
ステップ 7	show running-config section user-name 例 : Device # show running-config section guest	設定の詳細を表示します。

モビリティ エージェント (MA) の設定

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : Device # configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	wireless mobility controller ipmc-ipaddress public-ip mc-publicipaddress 例 : Device (config) # wireless mobility controller ip27.0.0.1 public-ip 27.0.0.1	MA が関連付けられるモビリティ コントローラを設定します。

	コマンドまたはアクション	目的
ステップ 3	wlan wlan-name wlan-id ssid 例 : Device (config) # wlan mywlan 34 mywlan-ssid	<ul style="list-style-type: none"> • <i>wlan-name</i> には、プロファイル名を入力します。範囲は 1 ~ 32 文字です。 • <i>wlan-id</i> には WLANID を入力します。範囲は 1 ~ 512 です。 • <i>ssid</i> では、この WLAN に対する Service Set Identifier (SSID) を入力します。SSID を指定しない場合、WLAN プロファイル名は SSID として設定されます。
ステップ 4	client vlan idvlan-group name/vlan-id 例 : Device (config-wlan) # client vlan VLAN0136	WLAN の VLAN ID またはグループを設定します。
ステップ 5	no security wpa 例 : Device (config-wlan) # no security wpa	セキュリティ設定は GC で作成された WLAN で同じである必要があります。この例はオープン認証を対象としています。オープンおよび webauth などの他のセキュリティタイプに対して、適切なコマンドを提供する必要があります。
ステップ 6	mobility anchor ipaddress 例 : Device (config-wlan) # mobility anchor 9.3.32.2	ゲスト コントローラをモビリティ アンカーとして設定します。
ステップ 7	aaa-override 例 : Device (config-wlan) # aaa-override	(任意) AAA オーバーライドをイネーブルにします。AAA オーバーライドは、AAA 属性を優先する必要がある場合のために、非オープン認証で要求されます。ゲストユーザの有効期限が切れた後に認証解除する必要があるか、AAA オーバーライド属性をユーザに与える必要がある場合にのみ必要です。
ステップ 8	no shutdown 例 : Device (config-wlan) # no shutdown	WLAN をイネーブルにします。
ステップ 9	end 例 : Device (config) # end	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 10	show wireless mobility summary 例： Device # show wireless mobility summary	モビリティコントローラの IP アドレス、およびモビリティトンネルのステータスを確認します。
ステップ 11	show wlan name wlan-name/id 例： Device # show wlan name mywlan	モビリティアンカーの設定を表示します。

モビリティコントローラの設定

モビリティコントローラモードは **wireless mobility controller** コマンドを使用してイネーブルにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device # configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	wireless mobility group member ip ip-address public-ip ip-address group group-name 例： Device (config) # wireless mobility group member ip 27.0.0.1 public-ip 23.0.0.1 group test	MCグループ内のすべてのピアを追加します。 <i>ip-address</i> は、ゲストコントローラの IP アドレスである必要があります。
ステップ 3	wireless mobility controller peer-group peer-group-name 例： Device (config) # wireless mobility controller peer-group pg	スイッチのピアグループを作成します。
ステップ 4	wireless mobility controller peer-group peer-group-name member ip ipaddress public-ip ipaddress 例： Device (config) # wireless mobility controller peer-group pg member ip 9.7.136.10 public-ip 9.7.136.10	スイッチのピアグループに MA を追加します。

	コマンドまたはアクション	目的
ステップ 5	end 例： Device (config) # end	特権 EXEC モードに戻ります。
ステップ 6	show wireless mobility summary 例： Device # show wireless mobility summary	設定の詳細を表示します。

Web 認証証明書の手入

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device # configure terminal	グローバルコンフィギュレーションモードを開始します。
ステップ 2	crypto pki import trustpoint name pkcs12 tftp: passphrase 例： Device (config)# crypto pki import cert pkcs12 tftp://9.1.0.100/ldapserver-cert.p12 cisco	証明書をインポートします。
ステップ 3	end 例： Device (config)# end	特権 EXEC モードに戻ります。
ステップ 4	show crypto pki trustpoints cert 例： Device # show crypto pki trustpoints cert	設定の詳細を表示します。

Web 認証証明書の表示

手順

	コマンドまたはアクション	目的
ステップ 1	show crypto ca certificate verb 例： Device # show crypto ca certificate verb	現在の Web 認証証明書の詳細を表示します。

デフォルトの Web 認証ログイン ページの選択

AAA オーバーライドフラグは、ローカルまたはリモート AAA サーバを使用した Web 認証のために、WLAN でイネーブルにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device # configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	parameter-map type webauth parameter-map name 例： Device (config) # parameter-map type webauth test	web-auth パラメータ マップを設定します。
ステップ 3	wlan wlan-name 例： Device (config) # wlan wlan10	wlan-name に、プロファイル名を入力します。範囲は 1 ~ 32 文字です。
ステップ 4	shutdown 例： Device (config) # shutdown	WLAN をディセーブルにします。
ステップ 5	security web-auth 例： Controller (config-wlan) # security web-auth	WLAN の Web 認証をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 6	security web-auth authentication-list <i>authentication list name</i> 例： Controller (config-wlan) # security web-auth authentication-list test	認証リスト名と Web 認証 WLAN のマップを可能にします。
ステップ 7	security web-auth parameter-map <i>parameter-map name</i> 例： Device (config) # security web-auth parameter-map test	パラメータ マップ名と Web 認証 WLAN のマップを可能にします。
ステップ 8	no shutdown 例： Device (config) # no shutdown	WLAN をイネーブルにします。
ステップ 9	end 例： Device (config) # end	特権 EXEC モードに戻ります。
ステップ 10	show running-config section wlan-name 例： Device# show running-config section mywlan	設定の詳細を表示します。
ステップ 11	show running-config section parameter-map type webauth parameter-map 例： Device# show running-config section parameter-map type webauth test	設定の詳細を表示します。

外部 Web サーバでのカスタマイズされた Web 認証ログイン ページの選択

AAA オーバーライドフラグは、ローカルまたはリモート AAA サーバを使用した Web 認証のために、WLAN でイネーブルにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device # configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	parameter-map type webauth global 例： Device (config) # parameter-map type webauth global	グローバル webauth タイプ パラメータを設定します。
ステップ 3	virtual-ip {ipv4 ipv6} ip-address 例： Device (config-params-parameter-map) # virtual-ip ipv4 1.1.1.1	仮想 IP アドレスを設定します。
ステップ 4	parameter-map type webauth parameter-map name 例： Device (config-params-parameter-map) # parameter-map type webauth test	webauth タイプ パラメータを設定します。
ステップ 5	type {authbypass consent webauth webconsent} 例： Device (config-params-parameter-map) # type webauth	consent、passthru、webauth、または webconsent など WebAuth のサブタイプを設定します。
ステップ 6	redirect [for-login on-success on-failure] URL 例： Device (config-params-parameter-map) # redirect for-login http://9.1.0.100/login.html	ログイン ページ、成功ページおよび失敗ページのリダイレクト URL を設定します。
ステップ 7	redirect portal {ipv4 ipv6} ip-address 例： Device (config-params-parameter-map) # redirect portal ipv4 23.0.0.1	外部ポータル の IPv4 アドレスを設定します。
ステップ 8	end 例： Device (config-params-parameter-map) # end	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 9	show running-config section parameter-map 例： Device # show running-config section parameter-map	設定の詳細を表示します。

WLAN ごとのログインページ、ログイン失敗ページ、およびログアウトページの割り当て

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device # configure terminal	グローバルコンフィギュレーションモードを開始します。
ステップ 2	parameter-map type webauth <i>parameter-map-name</i> 例： Device (config) # parameter-map type webauth test	webauth タイプ パラメータを設定します。
ステップ 3	custom-page login device <i>html-filename</i> 例： Device (config-params-parameter-map) # custom-page login device device flash:login.html	Web 認証カスタマイズログインページに対するファイル名を指定できます。
ステップ 4	custom-page login expired <i>html-filename</i> 例： Device (config-params-parameter-map) # custom-page login expired device flash:loginexpired.html	Web 認証カスタマイズログイン期限切れページに対するファイル名を指定することを可能にします。
ステップ 5	custom-page failure device <i>html-filename</i> 例： Device (config-params-parameter-map) # custom-page failure device device flash:loginfail.html	Web 認証カスタマイズログイン失敗ページに対するファイル名を指定できます。

	コマンドまたはアクション	目的
ステップ 6	custom-page success device <i>html-filename</i> 例： Device (config-params-parameter-map) # custom-page success device device flash:loginsuccess.html	Web 認証カスタマイズログイン成功ページに対するファイル名を指定できます。
ステップ 7	end 例： Device (config-params-parameter-map) # end	特権 EXEC モードに戻ります。
ステップ 8	show running-config section parameter-map type webauth <i>parameter-map</i> 例： Device (config) # show running-config section parameter-map type webauth test	設定の詳細を表示します。

AAA-Override の設定

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device # configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 2	wlan <i>wlan-name</i> 例： Device (config) # wlan ramban	<i>wlan-name</i> にはプロファイル名を入力します。範囲は 1 ~ 32 文字です。
ステップ 3	aaa-override 例： Device (config-wlan) # aaa-override	WLAN の AAA オーバーライドをイネーブルにします。
ステップ 4	end 例： Device (config-wlan) # end	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	show running-config section wlan-name 例： Device # show running-config section ramban	設定の詳細を表示します。

クライアントの負荷分散の設定

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device # configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	wlan wlan-name 例： Device (config)# wlan ramban	<i>wlan-name</i> にはプロファイル名を入力します。
ステップ 3	shutdown 例： Device (config-wlan)# shutdown	WLAN をディセーブルにします。
ステップ 4	mobility anchor ip-address1 例： Device (config-wlan) # mobility anchor 9.7.136.15	ゲスト コントローラをモビリティ アンカーとして設定します。
ステップ 5	mobility anchor ip-address2 例： Device (config-wlan) # mobility anchor 9.7.136.16	ゲスト コントローラをモビリティ アンカーとして設定します。
ステップ 6	no shutdown wlan 例： Device (config-wlan) # no shutdown wlan	WLAN をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 7	end 例： Device (config-wlan) # end	特権 EXEC モードに戻ります。
ステップ 8	show running-config section wlan-name 例： Device # show running-config section ramban	設定の詳細を表示します。

事前認証 ACL の設定

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	wlan wlan-name 例： Device (config)# wlan ramban	<i>wlan-name</i> にはプロファイル名を入力します。
ステップ 3	shutdown 例： Device (config-wlan)# shutdown	WLAN をディセーブルにします。
ステップ 4	ip access-group web preauthrule 例： Device (config-wlan)# ip access-group web preauthrule	認証前に適用する必要がある ACL を設定します。
ステップ 5	no shutdown 例： Device (config)# no shutdown	WLAN をイネーブルにします。
ステップ 6	end 例： Device (config-wlan)# end	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 7	show wlan name <i>wlan-name</i> 例： Device# show wlan name ramban	設定の詳細を表示します。

IOS ACL 定義の設定

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device # configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip access-list extended <i>access-list number</i> 例： Device (config) # ip access-list extended 102	拡張 IP アクセスリストを設定します。
ステップ 3	permit udp any eq <i>port number any</i> 例： Device (config-ext-nacl) # permit udp any eq 8080 any	宛先ホストを設定します。
ステップ 4	end 例： Device (config-wlan) # end	特権 EXEC モードに戻ります。
ステップ 5	show access-lists <i>ACL 番号</i> 例： Device # show access-lists 102	設定の詳細を表示します。

Webpassthrough の設定

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device # configure terminal	グローバルコンフィギュレーション モードを開始します。
ステップ 2	parameter-map type webauth <i>parameter-map name</i> 例： Device (config) # parameter-map type webauth webparalocal	webauth タイプ パラメータを設定します。
ステップ 3	type consent 例： Device (config-params-parameter-map) # type consent	WebAuth タイプを同意として設定します。
ステップ 4	end 例： Device (config-params-parameter-map) # end	特権 EXEC モードに戻ります。
ステップ 5	show running-config section parameter-map type webauth <i>parameter-map</i> 例： Device (config) # show running-config section parameter-map type webauth test	設定の詳細を表示します。

ゲスト アクセスの設定例

例：Lobby Ambassador アカウントの作成

次の例は、Lobby Ambassador アカウントを設定する方法を示しています。

```
Device# configure terminal
Device(config)# user-name lobby
Device(config)# type lobby-admin
Device(config)# password 0 lobby
Device(config)# end
Device# show running-config | section lobby
      user-name lobby
```

```

creation-time 1351118727
password 0 lobby
type lobby-admin

```

例 : Web 認証証明書の入手

次の例は、Web 認証証明書を取得する方法を示しています。

```

Device# configure terminal
Device(config)# crypto pki import cert pkcs12 tftp://9.1.0.100/ldapserver-cert.p12 cisco
Device(config)# end
Device# show crypto pki trustpoints cert
Trustpoint cert:
  Subject Name:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
    o=Cisco
    l=SanJose
    st=California
    c=US
  Serial Number (hex): 00
  Certificate configured.
Device# show crypto pki certificates cert
Certificate
  Status: Available
  Certificate Serial Number (hex): 04
  Certificate Usage: General Purpose
  Issuer:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
    o=Cisco
    l=SanJose
    st=California
    c=US
  Subject:
    Name: ldapserver
    e=rkannajr@cisco.com
    cn=ldapserver
    ou=WNBU
    o=Cisco
    st=California
    c=US
  Validity Date:
    start date: 07:35:23 UTC Jan 31 2012
    end   date: 07:35:23 UTC Jan 28 2022
  Associated Trustpoints: cert ldap12
  Storage: nvram:rkannajrcisc#4.cer

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 00
  Certificate Usage: General Purpose
  Issuer:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
    o=Cisco
    l=SanJose
    st=California
    c=US
  Subject:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
    o=Cisco
    l=SanJose
    st=California

```

```

c=US
Validity Date:
  start date: 07:27:56 UTC Jan 31 2012
  end   date: 07:27:56 UTC Jan 28 2022
Associated Trustpoints: cert ldap12 ldap
Storage: nvram:rkannajrcisc#0CA.cer

```

例 : Web 認証証明書の表示

次の例は、Web 認証証明書を表示する方法を示しています。

```

Device# show crypto ca certificate verb
Certificate
Status: Available
Version: 3
Certificate Serial Number (hex): 2A9636AC00000000858B
Certificate Usage: General Purpose
Issuer:
cn=Cisco Manufacturing CA
o=Cisco Systems
Subject:
Name: WS-C3780-6DS-S-2037064C0E80
Serial Number: PID:WS-C3780-6DS-S SN:FOC1534X12Q
cn=WS-C3780-6DS-S-2037064C0E80
serialNumber=PID:WS-C3780-6DS-S SN:FOC1534X12Q
CRL Distribution Points:
http://www.cisco.com/security/pki/crl/cmca.crl
Validity Date:
  start date: 15:43:22 UTC Aug 21 2011
  end   date: 15:53:22 UTC Aug 21 2021
Subject Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Signature Algorithm: SHA1 with RSA Encryption
Fingerprint MD5: A310B856 A41565F1 1D9410B5 7284CB21
Fingerprint SHA1: 04F180F6 CA1A67AF 9D7F561A 2BB397A1 0F5EB3C9
X509v3 extensions:
X509v3 Key Usage: F0000000
  Digital Signature
  Non Repudiation
  Key Encipherment
  Data Encipherment
X509v3 Subject Key ID: B9EEB123 5A3764B4 5E9C54A7 46E6EECA 02D283F7
X509v3 Authority Key ID: D0C52226 AB4F4660 ECAE0591 C7DC5AD1 B047F76C
Authority Info Access:
Associated Trustpoints: CISCO_IDEVID_SUDI
Key Label: CISCO_IDEVID_SUDI

```

例 : ゲスト ユーザ アカунトの設定

次の例は、ゲスト ユーザ アカунトを設定する方法を示しています。

```

Device# configure terminal
Device(config)# user-name guest
Device(config-user-name)# password 0 guest
Device(config-user-name)# type network-user description guest guest-user lifetime year 1
month 10 day 3 hour 1 minute 5 second 30
Device(config-user-name)# end
Device# show aaa local netuser all
User-Name      : guest
Type           : guest
Password       : guest
Is_passwd_encrypted : No

```

例 : モビリティ コントローラ の設定

```

Descriptio      : guest
Attribute-List  : Not-Configured
First-Login-Time : Not-Logged-In
Num-Login       : 0
Lifetime        : 1 years 10 months 3 days 1 hours 5 mins 30 secs
Start-Time      : 20:47:37 chennai Dec 21 2012

```

例 : モビリティ コントローラ の設定

次の例は、モビリティ コントローラ を設定する方法を示しています。

```

Device# configure terminal
Device(config)# wireless mobility group member ip 27.0.0.1 public-ip 23.0.0.1 group test
Device(config)# wireless mobility controller peer-group pg
Device(config)# wireless mobility controller peer-group pg member ip 9.7.136.10 public-ip
9.7.136.10
Device(config)# end
Device# show wireless mobility summary

```

Mobility Controller Summary:

```

Mobility Role           : Mobility Controller
Mobility Protocol Port  : 16666
Mobility Group Name     : default
Mobility Oracle         : Enabled
DTLS Mode               : Enabled
Mobility Domain ID for 802.11r : 0xac34
Mobility Keepalive Interval : 10
Mobility Keepalive Count : 3
Mobility Control Message DSCP Value : 7
Mobility Domain Member Count : 3

```

Link Status is Control Link Status : Data Link Status

Controllers configured in the Mobility Domain:

IP	Public IP	Group Name	Multicast IP	Link Status
9.9.9.2	-	default	0.0.0.0	UP : UP
12.12.11.11	12.13.12.12	rasagna-grp		DOWN : DOWN
27.0.0.1	23.0.0.1	test		DOWN : DOWN

```

Switch Peer Group Name      : spg1
Switch Peer Group Member Count : 0
Bridge Domain ID           : 0
Multicast IP Address        : 0.0.0.0

```

```

Switch Peer Group Name      : pg
Switch Peer Group Member Count : 1
Bridge Domain ID           : 0
Multicast IP Address        : 0.0.0.0

```

IP	Public IP	Link Status
9.7.136.10	9.7.136.10	DOWN : DOWN

例 : デフォルトの Web 認証ログイン ページ の選択

次の例は、デフォルトの Web 認証ログイン ページ を選択する方法を示しています。

```

Device# configure terminal
Device(config)# parameter-map type webauth test
This operation will permanently convert all relevant authentication commands to their CPL
control-policy equivalents. As this conversion is irreversible and will
disable the conversion CLI 'authentication display [legacy|new-style]', you are strongly

```

```

advised to back up your current configuration before proceeding.
Do you wish to continue? [yes]: yes
Device(config)# wlan wlan50
Device(config-wlan)# shutdown
Device(config-wlan)# security web-auth authentication-list test
Device(config-wlan)# security web-auth parameter-map test
Device(config-wlan)# no shutdown
Device(config-wlan)# end
Device# show running-config | section wlan50
wlan wlan50 50 wlan50
  security wpa akm cckm
  security wpa wpa1
  security wpa wpa1 ciphers aes
  security wpa wpa1 ciphers tkip
  security web-auth authentication-list test
  security web-auth parameter-map test
  session-timeout 1800
  no shutdown

Device# show running-config | section parameter-map type webauth test
parameter-map type webauth test
  type webauth

```

例：外部 Web サーバでのカスタマイズされた Web 認証ログイン ページの選択

次の例は、外部 Web サーバからカスタマイズされた Web 認証ログイン ページを選択する方法を示しています。

```

Device# configure terminal
Device(config)# parameter-map type webauth global
Device(config-params-parameter-map)# virtual-ip ipv4 1.1.1.1
Device(config-params-parameter-map)# parameter-map type webauth test
Device(config-params-parameter-map)# type webauth
Device(config-params-parameter-map)# redirect for-login http://9.1.0.100/login.html
Device(config-params-parameter-map)# redirect portal ipv4 23.0.0.1
Device(config-params-parameter-map)# end
Device# show running-config | section parameter-map
parameter-map type webauth global
virtual-ip ipv4 1.1.1.1
parameter-map type webauth test
type webauth
redirect for-login http://9.1.0.100/login.html
redirect portal ipv4 23.0.0.1
security web-auth parameter-map rasagna-auth-map
security web-auth parameter-map test

```

例：WLAN ごとのログイン ページ、ログイン失敗 ページ、およびログアウト ページの割り当て

次の例は、WLAN ごとのログイン割り当て、ログイン失敗、およびログアウト ページを割り当てる方法を示しています。

```

Device# configure terminal
Device(config)# parameter-map type webauth test
Device(config-params-parameter-map)# custom-page login device flash:loginsantosh.html
Device(config-params-parameter-map)# custom-page login expired device flash:loginexpire.html
Device(config-params-parameter-map)# custom-page failure device flash:loginfail.html
Device(config-params-parameter-map)# custom-page success device flash:loginsuccess.html

```

例 : AAA-Override の 設定

```

Device(config-params-parameter-map)# end
Device# show running-config | section parameter-map type webauth test
parameter-map type webauth test
type webauth
redirect for-login http://9.1.0.100/login.html
redirect portal ipv4 23.0.0.1
custom-page login device flash:loginsantosh.html
custom-page success device flash:loginsuccess.html
custom-page failure device flash:loginfail.html
custom-page login expired device flash:loginexpire.html

```

例 : AAA-Override の 設定

次の例は、AAA-Override を設定する例を示しています。

```

Device# configure terminal
Device(config)# wlan fff
Device(config-wlan)# aaa-override
Device(config-wlan)# end
Device# show running-config | section fff
wlan fff 44 fff
aaa-override
shutdown

```

例 : クライアントの負荷分散の設定

次の例は、クライアントの負荷分散を設定する方法を示しています。

```

Device# configure terminal
Device(config)# wlan fff
Device(config-wlan)# shutdown
Device(config-wlan)# mobility anchor 9.7.136.15
Device(config-wlan)# mobility anchor 9.7.136.16
Device(config-wlan)# no shutdown wlan
Device(config-wlan)# end
Device# show running-config | section fff
wlan fff 44 fff
aaa-override
shutdown

```

例 : 事前認証 ACL の設定

次の例は、事前認証 ACL を設定する方法を示しています。

```

Device# configure terminal
Device(config)# wlan fff
Device(config-wlan)# shutdown
Device(config-wlan)# ip access-group web preauthrule
Device(config-wlan)# no shutdown
Device(config-wlan)# end
Device# show wlan name fff

```

例 : IOS ACL 定義の設定

次に、IOS ACL 定義を設定する例を示します。

```
Device# configure terminal
Device(config)# ip access-list extended 102
Device(config-ext-nacl)# permit udp any eq 8080 any
Device(config-ext-nacl)# end
Device# show access-lists 102
Extended IP access list 102
  10 permit udp any eq 8080 any
```

例 : Webpassthrough の設定

次の例は、Webpassthrough を設定する方法を示しています。

```
Device# configure terminal
Device(config)# parameter-map type webauth webparalocal
Device(config-params-parameter-map)# type consent
Device(config-params-parameter-map)# end
Device# show running-config | section parameter-map type webauth test
parameter-map type webauth test
type webauth
redirect for-login http://9.1.0.100/login.html
redirect portal ipv4 23.0.0.1
```

ゲスト アクセスに関する追加情報

関連資料

関連項目	マニュアルタイトル
モビリティ CLI コマンド	『 <i>Mobility Command Reference, Cisco IOS XE 3SE (Cisco WLC 5700 Series)</i> 』
モビリティ設定	『 <i>Mobility Configuration Guide, Cisco IOS XE 3SE (Cisco WLC 5700 Series)</i> 』
セキュリティ CLI コマンド	『 <i>Security Command Reference, Cisco IOS Release 3SE (Cisco WLC 5700 Series)</i> 』
Catalyst 5700 シリーズワイヤレスコントローラの Web ベースの認証	『 <i>Security Configuration Guide, Cisco IOS Release 3SE (Cisco WLC 5700 Series)</i> 』
有線ゲスト アクセス設定およびコマンド	<i>Identity Based Networking Services</i>

標準および RFC

標準/RFC	Title
なし	-

MIB

MIB	MIB のリンク
なし	<p>選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャセットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。</p> <p>http://www.cisco.com/go/mibs</p>

シスコのテクニカル サポート

説明	Link
<p>シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。</p> <p>お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service (Field Notice からアクセス)、Cisco Technical Services Newsletter、Really Simple Syndication (RSS) フィードなどの各種サービスに加入できます。</p> <p>シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。</p>	<p>http://www.cisco.com/support</p>

ゲスト アクセスの機能履歴と情報

リリース	機能情報
Cisco IOS XE Release 3.2SE	この機能が導入されました。