統合

次のセクションでは、Cisco ISE でのワイヤレスセットアップの構成と、Cisco ISE 機能をサポートするためにスイッチおよびワイヤレスコントローラで必要な構成について説明します。

Wireless Setup について

Wireless Setup では、802.1X、ゲスト、および BYOD サービスのワイヤレス フローを容易にセットアップできます。また、適切な場合にはゲスト向けのポータルと BYOD サービス向けのポータルを設定およびカスタマイズするためのワークフローも提供されます。これらのワークフローでは、最も一般的な推奨設定が提供されるため、Cisco ISE で関連ポータル フローを設定するよりもシンプルです。Wireless Setup では、Cisco ISE とワイヤレスコントローラでユーザーが実行する必要のあるステップの多くが自動的に処理されるため、迅速に作業環境を構築できます。

フローのテストと開発に、Wireless Setup により作成された環境を使用できます。Wireless Setup 環境が稼働したら、Cisco ISE に切り替えることができます。これにより、拡張設定に対応できるようになります。Cisco ISE でのゲストサービスの設定についての詳細は、お使いの Cisco ISE バージョンの『ISE Administrators Guide』と Cisco コミュニティ サイト（https://community.cisco.com/t5/security-documents/ise-guest-amp-web-authentication/ta-p/3657224）を参照してください。Cisco ISE の Wireless Setup の設定と使用の詳細については、https://community.cisco.com/t5/security-documents/cisco-ise-secure-access-wizard-saw-guest-byod-and-secure-access/ta-p/3636602を参照してください。

（注） Cisco ISE Wireless Setup はベータソフトウェアです。実稼働ネットワークでは Wireless Setup を使用しないでください。

- Wireless Setup は、Cisco ISE の新規インストール後はデフォルトで無効になっています。Wireless Setup は、Cisco ISE CLI から **application configure ise** コマンド（オプション 17 を選択）を使用するか、または Cisco ISE GUI ホームページの右上隅にある [Wireless Setup] オプション（ ）を使用して有効にすることができます。
- Cisco ISE を以前のバージョンからアップグレードした場合、Wireless Setup は機能しません。Wireless Setup は新規 Cisco ISE のインストールでのみサポートされています。
- Wireless Setup はスタンドアロンノードでのみ機能します。
- Wireless Setup のインスタンスは一度に 1 つのみ実行します。一度に Wireless Setup を実行できるのは 1 人のみです。
- Wireless Setup を使用するには、ポート 9103 と 9104 が開いている必要があります。これらのポートを閉じるには、CLI を使用して Wireless Setup を無効にします。

- 一部のフローの実行後に Wireless Setup の新規インストールを開始する場合には、CLI コマンド **application reset-config ise** を使用できます。このコマンドは Cisco ISE 設定をリセットして Cisco ISE データベースをクリアしますが、ネットワーク定義を維持します。したがって、Cisco ISE と Wireless Setup をリセットするときに Cisco ISE を再インストールしてセットアップを実行する必要はありません。

  Wireless Setup を再び使用開始するには、次の手順を実行して Cisco ISE と Wireless Setup の両方の設定をリセットできます。

  - CLI で **application reset-config** を実行し、Cisco ISE のすべての設定をリセットします。新規インストールで Wireless Setup をテストしていた場合、このコマンドを実行すると、Cisco ISE で Wireless Setup によって行われた設定が削除されます。
  - CLI で **application configure ise** を実行し、**[18]Reset Config Wi-Fi Setup** を選択します。これにより、Wireless Setup 設定データベースの内容が消去されます。
  - ワイヤレスコントローラで、Wireless Setup によってワイヤレスコントローラに追加された設定が削除されます。ワイヤレスコントローラでの Wireless Setup の設定内容については、Wireless Setup フローによる Cisco ISE とワイヤレスコントローラの変更（13 ページ）を参照してください。

  Cisco ISE の新規インストール完了後に VM のスナップショットを作成しておくと、このステップは実行せずに済みます。

  CLI の詳細については、お使いの ISE バージョンの『Cisco Identity Services Engine CLI リファレンス ガイド』を参照してください。

- Wireless Setup を使用するには、Cisco ISE のネットワーク管理者ユーザーである必要があります。
- Wireless Setup を使用するには、少なくとも 2 つの CPU コアと 8 GB のメモリが必要です。
- Active Directory（AD）グループとユーザーのみがサポートされています。Wireless Setup で 1 つ以上のフローを作成すると、その他のタイプのユーザー、グループ、認証を Wireless Setup で使用できますが、それらを ISE で設定する必要があります。
- Cisco ISE で Active Directory をすでに定義しており、この AD を Wireless Setup に使用する予定の場合は、次の要件を満たしている必要があります。
  - 参加名とドメイン名が同一である必要があります。これらの名前が同一でない場合は、Wireless Setup でその AD を使用する前に、Cisco ISE で名前を同一にしてください。
  - ワイヤレスコントローラが Cisco ISE 上にすでに設定されている場合は、ワイヤレスコントローラに共有秘密が設定されている必要があります。ワイヤレスコントローラの定義に共有秘密がない場合は、Wireless Setup でそのワイヤレスコントローラを設定する前に共有秘密を追加するか、または Cisco ISE からワイヤレスコントローラを削除します。
- Wireless Setup では Cisco ISE コンポーネントを設定できますが、フローの開始後に Cisco ISE コンポーネントを削除または変更することはできません。Cisco ISE の Wireless Setup

で設定するすべての項目のリストについては、お使いの Cisco ISE バージョンの『Cisco Identity Services Engine CLI リファレンスガイド』を参照してください。

- 開始したフローは完了する必要があります。フローでトピックパスをクリックすると、フローが停止します。フローをステップに従って進むと、Cisco ISE 設定が動的に変更されます。Wireless Setup では設定変更のリストが表示されるので、手動で変更を元に戻すことができます。1つの例外を除いて、フローで前に戻って追加の変更を行うことはできません。例外として、ゲスト ポータルまたは BYOD ポータルのカスタマイズ内容を変更する場合には戻ることができます。
- 複数のワイヤレスコントローラと Active Directory ドメインがサポートされていますが、各フローでは 1 つのワイヤレスコントローラと 1 つの Active Directory のみがサポートされています。
- Wireless Setup には、Cisco ISE Basic ライセンスが必要です。BYOD には Cisco ISE Plus ライセンスが必要です。
- Wireless Setup の設定前に Cisco ISE リソースを設定している場合、Wireless Setup が既存のポリシーと矛盾することがあります。この状況では、Wireless Setup から、ツールの実行後に認証ポリシーをレビューするよう指示されます。Wireless Setup の実行時には、正常にセットアップされた Cisco ISE を使用して開始することが推奨されます。Wireless Setup と Cisco ISE の混在設定のサポートは限定されています。
- Wireless Setup は英語でのみ提供されており、他の言語では提供されていません。ポータルで他の言語を使用する場合には、Wireless Setup の実行後に Cisco ISE でその言語を設定してください。
- BYOD ではデュアル SSID がサポートされています。この設定で使用されるオープン SSID では、競合のためゲスト アクセスはサポートされません。ゲストと BYOD の両方に対応したポータルが必要な場合、Wireless Setup は使用できません。これについてはこのマニュアルでは説明しません。
- **電子メール通知と SMS 通知**
  - アカウント登録ゲストの場合、SMS 通知と電子メール通知がサポートされています。これらの通知は、ポータル カスタマイズ通知セクションで設定します。SMS 通知と電子メール通知をサポートするように SMTP サーバーを設定する必要があります。Cisco ISE に組み込まれているセルラープロバイダ（AT&T、T Mobile、Sprint、Orange、Verizon など）は、事前に設定されている無料の電子メール/SMS ゲートウェイです。
  - ゲストはポータルで各自のセルラープロバイダを選択します。プロバイダがリストにない場合は、メッセージを受信できません。グローバル プロバイダも設定できますが、これについてはこのマニュアルでは説明しません。ゲスト ポータルで SMS 通知と電子メール通知が設定されている場合、ゲストは両方のサービスの値を入力する必要があります。
  - Sponsored Guest フローでは、Wireless Setup での SMS 通知または電子メール通知の設定は行いません。このフローについては、Cisco ISE で通知サービスを設定する必要があります。

- ポータルで通知を設定するときには、SMS プロバイダ *Global Default* を選択しないでください。（デフォルトでは）このプロバイダは設定されていません。

- Wireless Setup では、HA を使用しないスタンドアロンセットアップだけがサポートされています。認証のために追加の PSN を使用する場合は、それらの PSN の Cisco ISE IP アドレスをワイヤレスコントローラの RADIUS 設定に追加してください。

Wireless Setup での Apple ミニブラウザ（Captive Network Assistant）のサポート

- **ゲストフロー**：Apple 擬似ブラウザの自動ポップアップは、すべてのゲストフローで機能します。ゲストは Apple の Captive Network Assistant ブラウザを使用してフローを通過することができます。Apple ユーザーが OPEN ネットワークに接続すると、ミニブラウザが自動的に表示されます。これにより、ユーザーは AUP（ホットスポット）を受け入れるか、または各自のクレデンシャルを使用してアカウント登録またはログインを実行できます。

- **BYOD**

  - **シングル SSID**：Cisco ISE リリース 2.2 では Apple ミニブラウザのサポートが追加されました。ただし Apple デバイスで SSID フローの問題が発生する可能性を抑えるため、リダイレクション ACL に captive.apple.com を追加してミニブラウザが表示されないようにしました。これにより、Apple デバイスはインターネットにアクセスできると想定します。ユーザーは、Web 認証またはデバイスオンボーディングのためにポータルにリダイレクトされるように、Safari ブラウザを手動で起動する必要があります。

  - **デュアル SSID**：ゲストアクセスを開始するか、または従業員がデバイスオンボーディング（BYOD）を実行できるようにするために、最初の OPEN ネットワーク WLAN で開始し、セキュア SSID にリダイレクトされるデュアル SSID フローの場合にも、ミニブラウザが表示されなくなります。

Apple CAN ミニブラウザの詳細については、https://communities.cisco.com/docs/DOC-71122 を参照してください。

ワイヤレスネットワークでのワイヤレスコントローラの設定

Wireless Setup を初めて起動してフローを選択すると、ワイヤレスコントローラを設定するように求められます。Wireless Setup では、設定するフローのタイプに対応するために必要な設定がワイヤレスコントローラにプッシュされます。

- ワイヤレスコントローラは、AireOS 8.x 以降を実行するシスコ ワイヤレス コントローラである必要があります。

- 仮想ワイヤレスコントローラは、DNS ベースの ACL をサポートしていません。

- Wireless Setup 展開で使用する予定のインターフェイス VLAN（ネットワーク）用にワイヤレスコントローラを設定します。デフォルトでは、ワイヤレスコントローラには管理イ

ンターフェイスがありますが、ゲストアクセスやセキュアアクセス（従業員）のネットワーク用に別のインターフェイスを設定することが推奨されます。

- ゲストフローの場合、AUP の受け入れ（ホットスポット）、ログイン、またはクレデンシャルの作成のために、ACL_WEBAUTH_REDIRECT ACL を使用して、ゲストデバイスがホットスポットまたはクレデンシャルを持つゲストポータルのいずれかにリダイレクトされます。承認されたゲストには、アクセスが許可されます（ACCESS-ACCEPT）。ワイヤレスコントローラの ACL を使用して、ゲストの権限を制限できます。これを行うには、ワイヤレスコントローラで ACL を作成し、ゲストのアクセス権の認証プロファイルでその ACL を使用します。Cisco ISE の成功ページへのアクセスを許可するには、この ACL をワイヤレスコントローラに追加します。限定的な ACL の作成の詳細については、https://communities.cisco.com/docs/DOC-68169 を参照してください。
- Wireless Setup ではフローごとに WLAN が設定されます。フローに WLAN を設定したら、その WLAN は他のフローには使用できません。唯一の例外は、アカウント登録フロー用に WLAN を設定しており、後でこの WLAN をスポンサーゲストフロー（ゲストのアカウント登録とスポンサー処理の両方を扱うフロー）に使用することに決定した場合です。

  実稼働環境で Wireless Setup を実行する場合、設定によって一部の既存ユーザーの接続が切断されることがあります。
- Wireless Setup でワイヤレスコントローラを使用してフローを設定する場合は、Cisco ISE でそのワイヤレスコントローラを削除しないでください。
- Cisco ISE ですでにワイヤレスコントローラを設定しているものの、RADIUS のオプションで共有秘密を設定しなかった場合は、Wireless Setup のそのワイヤレスコントローラを使用する前に、共有秘密を追加する必要があります。
- Cisco ISE でワイヤレスコントローラをすでに設定しており、共有秘密を設定している場合は、Wireless Setup で異なる共有秘密を設定しないでください。Wireless Setup と Cisco ISE のシークレットパスワードが一致している必要があります。選択する WLAN はフローで無効にされますが、フローの終わりで [本番稼働（Go Live）] ボタンをクリックすると再度有効にできます。
- **リモート LAN**：ネットワークにリモート LAN が含まれている場合、ワイヤイレスセットアップはリモート LAN にすでに割り当てられている VLAN ID を使用しようとすると失敗します。この回避策として、リモート LAN を削除するか、または Wireless Setup を実行する前にワイヤレスコントローラで使用する予定の VLAN を作成しておきます。Wireless Setup では、フローに対してこれらの既存の VLAN を有効にできます。
- **FlexConnect**：Flexconnect ローカルスイッチと Flexconnect ACL は Wireless Setup によって設定されますが使用されず、サポートされていません。Wireless Setup は、Flexconnect 集中型またはローカルモードのアクセスポイントと SSID でのみ動作します。

ワイヤレス設定の例

次に示すワイヤレスコントローラのログの一部分には、フローの設定時に Wireless Setup により行われる設定の例が示されています。

```
"config radius auth add 1 192.168.201.228 1812 ascii cisco"
"config radius auth disable 1"
"config radius auth rfc3576 enable 1"
"config radius auth management 1 disable"
"config radius auth enable 1"
"config radius acct add 1 192.168.201.228 1813 ascii cisco"
"config radius acct enable 1"
"config acl create ACL_WEBAUTH_REDIRECT"
"config acl rule add ACL_WEBAUTH_REDIRECT 1"
"config acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config acl rule source port range ACL_WEBAUTH_REDIRECT 1 53 53"
"config acl rule protocol ACL_WEBAUTH_REDIRECT 1 17"
"config acl rule add ACL_WEBAUTH_REDIRECT 1"
"config acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config acl rule destination port range ACL_WEBAUTH_REDIRECT 1 53 53"
"config acl rule protocol ACL_WEBAUTH_REDIRECT 1 17"
"config acl rule add ACL_WEBAUTH_REDIRECT 1"
"config acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config acl rule source address ACL_WEBAUTH_REDIRECT 1 192.168.201.228 255.255.255.255"
"config acl rule add ACL_WEBAUTH_REDIRECT 1"
"config acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config acl rule destination address ACL_WEBAUTH_REDIRECT 1 192.168.201.228
255.255.255.255"
"config acl apply ACL_WEBAUTH_REDIRECT"
"show flexconnect acl summary"
"config flexconnect acl create ACL_WEBAUTH_REDIRECT"
"config flexconnect acl rule add ACL_WEBAUTH_REDIRECT 1"
"config flexconnect acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config flexconnect acl rule source port range ACL_WEBAUTH_REDIRECT 1 53 53"
"config flexconnect acl rule protocol ACL_WEBAUTH_REDIRECT 1 17"
"config flexconnect acl rule add ACL_WEBAUTH_REDIRECT 1"
"config flexconnect acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config flexconnect acl rule destination port range ACL_WEBAUTH_REDIRECT 1 53 53"
"config flexconnect acl rule protocol ACL_WEBAUTH_REDIRECT 1 17"
"config flexconnect acl rule add ACL_WEBAUTH_REDIRECT 1"
"config flexconnect acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config flexconnect acl rule source address ACL_WEBAUTH_REDIRECT 1 192.168.201.228
255.255.255.255"
"config flexconnect acl rule add ACL_WEBAUTH_REDIRECT 1"
"config flexconnect acl rule action ACL_WEBAUTH_REDIRECT 1 permit"
"config flexconnect acl rule destination address ACL_WEBAUTH_REDIRECT 1 192.168.201.228
 255.255.255.255"
"config flexconnect acl apply ACL_WEBAUTH_REDIRECT"
```

Active Directory と Wireless Setup

スポンサーゲスト、802.1x、およびBYODのフローを作成するには、Active Directoryドメインが必要です。Active Directoryは、スポンサーポータル、802.1xセキュアアクセスおよび関連VLAN、BYODおよびデバイスオンボーディングにアクセスできるスポンサーグループのユーザーを指定します。Wireless Setupでいずれかのフローを設定したら、必要に応じて[Cisco ISEアイデンティティ（Cisco ISE Identities）]に移動して次の項目を追加できます。

- スポンサーグループにマッピングされている内部スポンサーアカウント（ALL_ACCOUNTSなど）。Active Directoryを使用している場合は、これは不要です。
- Cisco ISE内部従業員グループに含まれている従業員。内部従業員グループが認証ポリシーに追加されていることを確認します。

Wireless Setup でのゲスト ポータル

企業の訪問者が企業のネットワークを使用してインターネットまたはネットワーク上のリソースおよびサービスにアクセスしようとしている場合、ゲストポータルを使用してネットワークアクセスを提供することができます。設定すると、従業員はゲストポータルを使用して会社のネットワークにアクセスできます。

3 つのデフォルトのゲスト ポータルがあります。

- [ホットスポットゲストポータル（Hotspot Guest portal）]：ネットワークアクセスはログイン情報を必要とせずに許可されます。通常、ネットワーク アクセスを許可する前にユーザー ポリシーの認可（AUP）が承認される必要があります。
- [Sponsored-Guest ポータル（Sponsored-Guest portal）]：ゲストのアカウントを作成したスポンサーによりネットワークアクセスが許可され、ゲストにログイン情報が提供されます。
- [アカウント登録ゲストポータル（Self-Registered Guest portal）]：ゲストは各自のアカウントのログイン情報を作成できます。ネットワークアクセスが付与される前に、スポンサー承認が必要となることがあります。

Cisco ISE は、事前に定義されたデフォルト ポータルなど、複数のゲスト ポータルをホストすることができます。

デフォルトのポータル テーマには、管理者ポータルからカスタマイズできる標準のシスコ ブランドが適用されています。

Wireless Setup には独自のデフォルトテーマ（CSS）があります。ロゴ、バナー、背景画像、色、フォントなどの基本的な設定の一部を変更できます。ISE では、他の設定を変更することでポータルをさらにカスタマイズでき、高度なカスタマイズを行うこともできます。

ゲスト ポータル ワークフロー

1. ポータルのタイプを選択すると、使用するコントローラを選択するよう求められます。フローごとに新しいワイヤレス ネットワークを設定します。Wireless Setup でまだ使用していない既存の WLAN を選択するか、または新しい WLAN を作成することができます。

   リダイレクトが必要なフローには、発信元 URL、成功ページ、または特定の URL（www.cisco.com など）にユーザーをリダイレクトするオプションがあります。発信元 URL はワイヤレスコントローラからサポートする必要があります。

（注） 発信元 URL はワイヤレスコントローラのバージョン 8.4 以降でサポートされています。

2. ポータルの外観をカスタマイズし、基本設定を変更します。
3. カスタマイズが完了したら、テスト ポータルへの URL リンクをたどります。テスト ポータルに、ポータルのテストバージョンのプレビューが表示されます。フローを通過し、必要に応じてさらに変更を行うことができます。機能する正常なリダイレクトのみが成功

ページの対象であることに注意してください。発信元 URL と静的 URL はテストポータルでは機能しません。これらの URL はリダイレクトのサポートにワイヤレスセッションが必要であるためです。テストポータルはRADIUS セッションをサポートしていません。そのため、ポータルフロー全体は表示されません。複数の PSN がある場合、Cisco ISE は最初のアクティブ PSN を選択します。

4. これで設定が完了しました。ワークフロー時にWireless Setup によって Cisco ISE とワイヤレスコントローラで実行されたステップをダウンロードして表示できます。

（注） Wireless Setup では基本ゲスト アクセスにはロケーションは使用されません。ローカル時刻に基づいてアクセスを制御する場合に、ロケーションが必要となります。Cisco ISE でのタイムゾーンの設定については、SMS プロバイダおよびサービスを参照してください。

ワイヤレス ネットワーク アカウント登録ポータル

アカウント登録ゲスト ポータルでは、ゲストが自分自身を登録し、自分のアカウントを作成して、ネットワークにアクセスできるようにすることができます。

ログオン成功ページではユーザーに対して画面にログオンクレデンシャルが表示されるため、ログオン成功ページを選択しないことをお勧めします。ベストプラクティスは、電子メールまたはSMS を介してユーザークレデンシャルを取得することです。それによって、クレデンシャルが監査目的に特有の内容に関連付けられます。

ワイヤレス ネットワーク Sponsored Guest フロー

スポンサーはスポンサーポータルを使用して、承認ユーザー用の一時アカウントを作成および管理し、企業ネットワークまたはインターネットにセキュアにアクセスできるようにします。ゲスト アカウントを作成した後、スポンサーは、スポンサー ポータルを使用して、印刷、電子メール送信、または携帯電話による送信を行ってゲストにアカウントの詳細を提供することもできます。アカウント登録ゲストに企業ネットワークへのアクセス権を提供する前に、スポンサーはゲストアカウントを承認するように電子メールで要求されることがあります。

スポンサーフロー時に、Wireless Setup がスポンサーポータルとスポンサーゲストポータルを設定します。

承認フローは Wireless Setup ではサポートされていません。

ワークフロー時に Active Directory グループをスポンサーグループにマッピングします。ワークフローにより、選択された AD グループが ALL_ACCOUNTS スポンサー グループにマッピングされます。GROUP または OWN アカウント スポンサー グループは設定されません。必要に応じて、他のアイデンティティソース（内部設定や LDAP 設定など）を追加するには、Cisco ISE 管理 UI を使用して追加できます。詳細については、「スポンサー グループ」を参照してください。

Wireless Setup BYOD フロー：ネイティブ サプリカントおよび証明書のプロビジョニング

個人所有デバイスの持ち込み（BYOD）ポータルでは、従業員が各自のパーソナルデバイスを登録できます。ネイティブ サプリカント、証明書プロビジョニングはネットワークへのアクセスを許可する前にすることができます。従業員はBYODポータルに直接アクセスできません。パーソナルデバイスを登録するときにこのポータルにリダイレクトされます。従業員がパーソナルデバイスを使用してネットワークへ初めてアクセスしようとすると、（iOS以外のデバイスの場合）手動でNetwork Setup Assistant（NSA）ウィザードをダウンロードして起動するように促されることがあります。NSA では、ネイティブ サプリカントの登録とインストールを順を追って実行できます。デバイスを登録すると、デバイス ポータルを使用して、それを管理できます。

Wireless Setup は Cisco ISE とコントローラでネイティブサプリカントと証明書のプロビジョニングを設定します。ユーザーはコントローラに PEAP 接続し、証明書を提供します。接続が EAP-TLS（証明書）に切り替わります。

Wireless Setup でサポートされるデバイスは、Apple デバイス（MAC および iOS）、Windows デスクトップ OS（モバイル以外）、および Android です。Chrome OS オンボーディングは、Wireless Setup ではサポートされていません。

Android デバイスの場合は、シングルまたはデュアル EAP-TLS ベースの BYOD フローが正常に動作するために、基本認証アクセスポリシーが有効になっていることを確認します。**[ポリシー（Policy）] > [プリシーセット（Policy Sets）] > [デフォルト（Default）] > [認証ポリシー（Authorization Policy）]**に移動し、**Basic_Authenticated_Access** がアクティブであることを確認します。

（注） デュアルSSIDフローは、オンボーディング用のオープン ネットワークと、認証済みアクセス用の TLS 証明書ベースのセキュア ネットワークで構成されます。デバイスはオンボーディングなしでセキュア ネットワークに接続できます。これは、**Basic_Authenticated_Access** デフォルトルールにより有効な認証はすべて通過できるためです。デバイスがセキュアなネットワークに接続する際に、BYOD セキュア許可ルールに一致しないと、**Basic_Authenticated_Access** ルールのリストの下部に一致が移動します。

この対策として、許可ポリシーで **Basic_Authenticated_Access** ルールを無効にするか、または特定の SSID（WLAN）に一致するようにこのルールを編集します。いずれの変更でも、許可しないデバイスへの PEAP 接続がブロックされます。

（注） Wireless Setup には、ロストとマークされたデバイスをリダイレクトする認証ルールはありません。これは、デバイスをブロックすることで実行され、ブラックリストポータルによって管理されます。ロストしたデバイスや盗まれたデバイスの管理については、http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide/Managing_Lost_or_Stolen_Device.pdf を参照してください。

Wireless Setup での BYOD フロー

Wireless Setup での BYOD 設定は次のステップで構成されます。

1. ワイヤレス LAN コントローラを選択または登録します。
2. ワイヤレスネットワークを追加します。

（注） 新しい Cisco ISE インストールには、デフォルトのワイヤレスネットワークが含まれます。デュアル SSID BYOD では、ユーザーが 2 番目の SSID にリダイレクトされると、ユーザーのネットワーク プロファイルにデフォルトのネットワーク SSID が示されます。デフォルト SSID を削除するか、またはユーザーにこの SSID を無視するように通知できます。

3. Cisco ISE の選択または Active Directory（AD）への参加：オンボーディング VLAN と最終アクセス VLAN の両方のデフォルト VLAN 設定を上書きできます。最終アクセス VLAN は Active Directory グループにマッピングされます。
4. BYOD ポータルのカスタマイズ：BYOD ポータルとデバイスポータルをここでカスタマイズできます。このステップでは、Cisco ISE がサポートするすべてのページをカスタマイズできます。このステップでは、すべてのポータルカスタマイズ内容が送信され、ポリシーが作成され、プロファイルが関連するポリシーにリンクされます。

（注） デバイスポータルは、BYOD ポータルカスタマイズの基本的なカスタマイズを使用します。Wireless Setup で My Devices ポータルをカスタマイズすることはできません。

5. 行った設定変更をプレビューして [完了（Done）] をクリックします。

デュアル SSID BYOD の場合

デュアル SSID BYOD をサポートするには、Fast SSID が有効になっている必要があります。ワイヤレスコントローラで Fast SSID Change が有効になっている場合、クライアントは SSID 間を高速で移動できます。高速 SSID が有効になっている場合、クライアント エントリがクリアされず、遅延は適用されません。シスコ ワイヤレス コントローラでの高速 SSID の構成に関する詳細については、『Cisco Wireless Controller Configuration Guide』を参照してください。

推奨される WLC タイマー設定

Wireless Setup で使用する予定のワイヤレスコントローラで次のコマンドを設定することをお勧めします。

```
config radius auth retransmit-timeout {SERVER_INDEX} 5
config radius aggressive-failover disable
config radius fallback-test mode passive
config wlan exclusionlist {WLAN ID} 180
config wlan exclusionlist {WLAN ID} enabled
```

802.1X ワイヤレス フロー

ワイヤレスセットアップフローにより、802.1x ワイヤレスコントローラが PEAP（ユーザー名とパスワードのクレデンシャル）を使用して設定されます。

このフローの一部で、Active Directory（AD）を指定するように求められます。従業員 AD グループを VLAN にマッピングできます。VLAN によってグループを分ける場合は、異なる従業員グループを異なる VLAN に設定することができます。[アクセス（Access）] の横のドロップダウンをクリックすると、設定した AD で使用可能な AD グループが表示されます。

Wireless Setup で AD グループを選択すると、各グループが VLAN にマッピングされます。AD グループが VLAN にマッピングされていない場合は、有効な AD ユーザーに対してログインを許可する基本アクセス ポリシーにユーザーが一致します。

従業員がネットワークに接続する

1. **従業員のクレデンシャルが認証される**：Cisco ISE は、社内 Active Directory と照合して従業員を認証し、認証ポリシーを提供します。
2. **デバイスが BYOD ポータルにリダイレクトされる**：デバイスが BYOD ポータルにリダイレクトされます。デバイスの [MACアドレス（MAC address）] フィールドが入力され、ユーザーはデバイス名と説明を追加できます。
3. **ネイティブサプリカントが設定される（MacOS、Windows、iOS、Android）**：ネイティブサプリカントが設定されます。ただしこのプロセスはデバイスに応じて異なります。
   - MacOS および Windows デバイス：従業員は BYOD ポータルで [登録（Register）] をクリックして、サプリカント プロビジョニング ウィザードをダウンロードしてインストールします。このウィザードは、サプリカントを設定し、EAP-TLS 証明書ベースの認証用の証明書をインストールします。デバイスの MAC アドレスと従業員のユーザー名が発行済み証明書に組み込まれます。

（注） MacOS の場合、Apple 証明書を除き、証明書は MacOS に [未署名（unsigned）] と表示されます。これは BYOD フローには影響しません。

- iOS デバイス：Cisco ISE ポリシーサーバーは Apple の iOS ワイヤレス機能を使用して新しいプロファイルを iOS デバイスに送信します。このプロファイルには次の情報が含まれます。
  - 発行された証明書が、IOS デバイスの MAC アドレスおよび従業員のユーザー名と共に保存されます。
  - 802.1X 認証の MSCHAPv2 または EAP-TLS の使用を強制できる Wi-Fi サプリカント プロファイル。
- Android デバイス：Cisco ISE は、従業員に Google Play ストアから Cisco Network Setup Assistant（NSA）をダウンロードするように要求し、ルーティングします。アプリのインストール後に、従業員はNSA を開いてセットアップ ウィザードを開始できます。スタートアップ ウィザードでは、サプリカントの設定と、デバイスの設定に使用される発行済み証明書が生成されます。
- **認可変更が発行される**：ユーザーがオンボーディングフローを通過すると、Cisco ISE は認可変更（CoA）を開始します。これにより、MacOSX、Windows、および Android デバイスは EAP-TLS を使用してセキュアな 802.1X ネットワークに再接続します。シングル SSID の場合、iOS デバイスも自動的に接続されますが、デュアル SSID の場合、ウィザードは iOS ユーザーに手動で新しいネットワークに接続するように要求します。

ネイティブ サプリカントは、次のオペレーティング システムでサポートされます。

- Android（Amazon Kindle、B&N Nook を除く）
- MacOS（Apple Mac コンピュータの場合）
- Apple iOS デバイス（Apple iPod、iPhone、および iPad）
- Microsoft Windows 7、8（RT を除く）、Vista、および 10

Wireless Setup フローによる Cisco ISE とワイヤレスコントローラの変更

Wireless Setup では、フローをステップに従って進むことで Cisco ISE とコントローラが設定されます。Wireless Setup は、行った変更のリストを各フローの終わりで表示します。各フローの変更内容がここで参考のために表示されます。これにより、Wireless Setup が Cisco ISE に対して行ったすべての変更を確認し、変更内容をレビューまたは変更できます。

- **ホットスポット**
  - **[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲストポータル（Guest Portals）] > [ホットスポットポータル（Hotspot Portal）]**

- **[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可プロファイル（Authorization Profiles）]**
- **[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポリシーセット（Policy Sets）]**

• アカウント登録

- **[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲストポータル（Guest Portals）] > [アカウント登録ポータル（Self-reg Portal）]**
- **[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲストタイプ（Guest Types）] > [ゲストタイプ（Guest Types）]**
- **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [許可（Authorization）] > [認証プロファイル（Authorization Profiles）]**
- **[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポリシーセット（Policy Sets）]**
- **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [SMTP サーバー（SMTP Server）]**
- **[管理（Administration）] > [システム（System）] > [設定（Settings）] > [SMTP ゲートウェイ（SMTP Gateway）]**

• スポンサー

- **[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲストポータル（Guest Portals）] > [スポンサーゲストポータル（Sponsored Guest Portal）] >**
- **[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサーポータル（Sponsor Portals）] > > [スポンサーポータル（Sponsor Portal）] >**
- **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [許可（Authorization）] > [認証プロファイル（Authorization Profiles）]**
- **[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [認証ポリシー（Authorization Policy）]**
- **[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [スポンサー（Sponsor）] > [スポンサーグループ（Sponsor Groups）]**
- **[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [ポータルとコンポーネント（Portals & Components）] > [ゲストタイプ（Guest Types）] > [ゲストタイプ（Guest Types）]**

- **[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [外部 ID ソース（Ext ID Sources）] > [Active Directory]**

- **BYOD**
  - **[ワークセンター（Work Centers）] > [BYOD] > [ポータルとコンポーネント（Portals & Components）] > [BYOD ポータル（BYOD Portals）] > [BYOD ポータル（BYOD Portal）]**
  - **[ワークセンター（Work Centers）] > [BYOD] > [ポータルとコンポーネント（Portals & Components）] > [デバイスポータル（My Devices Portals）] > [デバイスポータル（My Devices Portal）]**
  - **[ワークセンター（Work Centers）] > [BYOD] > [ポリシー要素（Policy Elements）] > [許可（Authorization）] > [認証プロファイル（Authorization Profiles）]**
  - **[ワークセンター（Work Centers）] > [BYOD] > [認証ポリシー（Authorization Policy）]**
  - **[ワークセンター（Work Centers）] > [BYOD] > [外部 ID ソース（Ext ID Sources）] > [Active Directory]**
  - **[ワークセンター（Work Centers）] > [BYOD] > [外部 ID ソース（Ext ID Sources）] > [Active Directory]** を選択し、AD を選択し、[グループ（Groups）] タブを選択します。

- セキュアなアクセス
  - **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可（Authorization）] > [認証プロファイル（Authorization Profiles）]**
  - **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可（Authorization）] > [認証プロファイル（Authorization Profiles）]**
  - **[ポリシー（Policy）] > [ポリシーセット（Policy Sets）]**
  - **[ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [外部 ID ソース（Ext ID Sources）] > [Active Directory]** を選択し、AD を選択して [グループ（Groups）] タブを選択します。

- ワイヤレス LAN コントローラ
  - **WLAN**
  - **[セキュリティ（Security）] > [アクセス制御リスト（Access Control Lists）]**：Wireless Setup では次の ACL が作成されます。
    - ゲストと BYOD 用のリダイレクト ACL
  - Wireless Setup により、**[セキュリティ（Security）] > [AAA] > [認証およびアカウンティング（Authentication and Accounting）]** にもエントリが作成されます。

スイッチでの標準 Web 認証のサポートの有効化

認証時の URL リダイレクションのプロビジョニングなど、Cisco ISE 用の標準 Web 認証機能を有効にするには、次のコマンドをスイッチの構成に含めます。

```
ip classless

ip route 0.0.0.0 0.0.0.0 10.1.2.3

ip http server
! Must enable HTTP/HTTPS for URL-redirection on port 80/443
ip http secure-server
```

代理 RADIUS トランザクション用のローカル ユーザー名とパスワードの定義

スイッチがこのネットワーク セグメントの RADIUS サーバーであるかのように Cisco ISE ノードと通信するには、次のコマンドを入力します。

```
username test-radius password 0 abcde123
```

ログとアカウンティングのタイムスタンプの正確性を保証するための NTP サーバー設定

次のコマンドを入力して、Cisco ISE で設定したものと同じ NTP サーバーをスイッチ上に指定していることを確認します。

```
ntp server <IP_address>|<domain_name>
```

AAA 機能を有効にするコマンド

802.1X および MAB 認証機能など、スイッチと Cisco ISE との間でさまざまな AAA 機能を有効にするには、スイッチ上で次のコマンドを入力します。

```
aaa new-model
! Creates an 802.1X port-based authentication method list
aaa authentication dot1x default group radius
```

```
! Required for VLAN/ACL assignment
aaa authorization network default group radius
! Authentication & authorization for webauth transactions
aaa authorization auth-proxy default group radius
! Enables accounting for 802.1X and MAB authentications
aaa accounting dot1x default start-stop group radius
!
aaa session-id common
!
aaa accounting update periodic 5
! Update AAA accounting information periodically every 5 minutes
aaa accounting system default start-stop group radius
!
```

スイッチ上の RADIUS サーバーの設定

Cisco ISE とやり取りし、RADIUS ソース サーバーとして動作するようスイッチを設定するには、次のコマンドを入力します。

```
!
radius-server <ISE Name>
! ISE Name is the name of the ISE PSN
address ipv4 <ip address> auth-port 1812 acct-port 1813
! IP address is the address of the PSN. This example uses the standard RADIUS ports.
key <passwd>
! passwd is the secret password confiugured in Cisco ISE
exit
```

（注） 3 回の再試行を含む 30 秒のデッド基準時間を設定し、Active Directory を認証に使用する RADIUS 要求に対して、より長い応答時間を提供することを推奨します。

RADIUS 許可変更（CoA）を有効にするコマンド

スイッチが RADIUS CoA 動作を適切に処理し、Cisco ISE でポスチャ機能をサポートできるようにするための設定を指定するには、次のコマンドを入力します。

```
aaa server radius dynamic-author

client <ISE-IP> server-key 0 abcde123
```

（注）

- Cisco ISE では、RFC の CoA 用デフォルト ポート 3799 に対して、ポート 1700（Cisco IOS ソフトウェアのデフォルト）を使用します。既存の Cisco Secure ACS 5.x ユーザーは、既存の ACS の実装の一部として CoA を使用している場合、すでにこれをポート 3799 に設定している可能性があります。
- 共有秘密キーは、ネットワークデバイスの追加時に Cisco ISE で設定したものと同じである必要があり、IP アドレスは PSN IP アドレスである必要があります。

デバイス トラッキングと DHCP スヌーピングを有効にするコマンド

セキュリティに関連する Cisco ISE のオプション機能を提供できるようにするには、次のコマンドを入力することによって、デバイス トラッキングと DHCP スヌーピングを有効にし、スイッチ ポートのダイナミック ACL 内で IP 置換を実現します。

```
! Optional

ip dhcp snooping

! Required!

! Configure Device Tracking Policy!
device-tracking policy <DT_POLICY_NAME>
no protocol ndp
tracking enable

! Bind it to interface!
interface <interface_id>
device-tracking attach-policy<DT_POLICY_NAME>
```

RADIUS アカウンティングでは、DHCP スヌーピングが有効になっていても、DHCP 属性は IOS センサーによって Cisco ISE に送信されません。このような場合、DHCP スヌーピングを VLAN で有効にして DHCP をアクティブにする必要があります。

VLAN で DHCP スヌーピングを有効にするには、次のコマンドを使用します。

```
ip dhcp snooping
```

```
ip dhcp snooping vlan 1-100
```

802.1X ポートベースの認証を有効にするコマンド

スイッチ ポートに対してグローバルに 802.1X 認証を有効にするには、次のコマンドを入力します。

```
dot1x system-auth-control
```

クリティカルな認証の EAP を有効にするコマンド

サプリカントによる LAN 経由での認証要求をサポートするには、次のコマンドを入力することによって、EAP をクリティカルな認証（アクセスできない認証バイパス）に対して有効にします。

```
dot1x critical eapol
```

リカバリ遅延を使用して AAA 要求をスロットリングするコマンド

クリティカルな認証リカバリイベントが発生した場合、次のコマンドを入力することで、自動的に遅延（秒単位）を発生させるようにスイッチを設定し、リカバリ後に Cisco ISE がサービスを再起動できるようにします。

```
authentication critical recovery delay 1000
```

適用状態に基づく VLAN の定義

ネットワーク内の既知の適用状態に基づいて VLAN 名、番号、およびスイッチ仮想インターフェイス（SVI）を定義するには、次のコマンドを入力します。ネットワーク間のルーティングを有効にするには、それぞれの VLAN インターフェイスを作成します。これは特に、エンドポイントがネットワークに接続するときに経由するエンドポイント（PC やラップトップ）と IP 電話の両方からの同じネットワークセグメントを経由して渡される複数のソースからのトラフィックを処理する場合に役立ちます。次に例を示します。

```
vlan <VLAN_number>

name ACCESS!

vlan <VLAN_number>
```

```
name VOICE
!
interface <VLAN_number>
description ACCESS
ip address 10.1.2.3 255.255.255.0
ip helper-address <DHCP_Server_IP_address>
ip helper-address <Cisco_ISE_IP_address>
!
interface <VLAN_number>
description VOICE
ip address 10.2.3.4 255.255.255.0
ip helper-address <DHCP_Server_IP_address>
```

スイッチでのローカル（デフォルト）アクセスリスト（ACL）の定義

このような機能を古いバージョンのスイッチ（Cisco IOS ソフトウェア リリースのバージョンが 12.2(55)SE よりも前）で有効にし、Cisco ISE が認証と許可に必要なダイナミック ACL の更新を実行できるようにするには、次のコマンドを入力します。

```
ip access-list extended ACL-ALLOW
 permit ip any any
!
ip access-list extended ACL-DEFAULT
  remark DHCP
  permit udp any eq bootpc any eq bootps
  remark DNS
  permit udp any any eq domain
```

```
  remark Ping
  permit icmp any any
  remark Ping
  permit icmp any any
  remark PXE / TFTP
  permit udp any any eq tftp
  remark Allow HTTP/S to ISE and WebAuth portal
permit tcp any host <Cisco_ISE_IP_address> eq www

permit tcp any host <Cisco_ISE_IP_address> eq 443

permit tcp any host <Cisco_ISE_IP_address> eq 8443

permit tcp any host <Cisco_ISE_IP_address> eq 8905

permit udp any host <Cisco_ISE_IP_address> eq 8905

permit udp any host <Cisco_ISE_IP_address> eq 8906

permit tcp any host <Cisco_ISE_IP_address> eq 8080

permit udp any host <Cisco_ISE_IP_address> eq 9996

remark Drop all the rest
  deny ip any any log
!
```

```
! The ACL to allow URL-redirection for WebAuth
ip access-list extended ACL-WEBAUTH-REDIRECT
 permit tcp any any eq www
 permit tcp any any eq 443
```

（注） ワイヤレスコントローラでこの設定を行うと、CPU 使用率が増加し、システムが不安定になるリスクが高まります。これは IOS の問題で、Cisco ISE は悪影響を受けません。

802.1X および MAB のスイッチ ポートを有効にする

802.1X および MAB のスイッチ ポートを有効にするには、以下の手順を実行します。

ステップ 1 すべてのアクセススイッチポートのインターフェイス コンフィギュレーション モードを開始します。
interface range FastEthernet0/1-8

ステップ 2 次のように、（トランク モードではなく）アクセス モードのスイッチ ポートを有効にします。
switchport mode access

ステップ 3 静的にアクセス VLAN を設定します。アクセス VLAN のローカル プロビジョニングを提供するこの手順は、オープンモード認証に必要となります。
switchport access vlan <*VLAN_number*>

ステップ 4 静的に音声 VLAN を設定します。
switchport voice vlan <*VLAN_number*>

ステップ 5 オープン モード認証を有効にします。オープン モードを使用すると、認証が完了する前に、トラフィックをデータおよび音声 VLAN 上にブリッジングできます。実稼働環境では、ポートベースの ACL を使用して不正アクセスを防ぐことを強く推奨します。
オープンモード認証を有効にすると、ポート ACL に従って AAA サーバー応答の前に事前認証アクセスも有効になります。
authentication open

ステップ 6 ポートベースの ACL を適用して、認証されていないエンドポイントからアクセス VLAN 上にデフォルトでどのトラフィックをブリッジングするかを決定します。最初にすべてのアクセスを許可してからポリシーを適用する必要があるため、ACL-ALLOW を適用して、スイッチ ポートを通過するすべてのトラフィックを許可する必要があります。すでに現時点のすべてのトラフィックを許可するデフォルトの Cisco ISE 許可を作成しましたが、この理由は、完全な可視性を実現し、既存のエンドユーザー環境にはまだ影響を与えないようにするためです。
ACL は AAA サーバーから動的 ACL の前に追加されるように設定する必要があります。
ip access-group ACL-ALLOW in

（注） DSBU スイッチ上に Cisco IOS Release 12.2(55)SE ソフトウェアを用意する前に、RADIUS AAA サーバーからのダイナミック ACL を適用するためのポート ACL が必要です。デフォルトの ACL を用意できなかった場合、割り当てられた動的 ACL はスイッチによって無視されます。Cisco IOS ソフトウェアのリリース 12.2(55)SE では、デフォルトの ACL が自動的に生成および適用されます。

（注） テストの現段階では、ポートベースの 802.1X 認証を有効にし、さらに既存のネットワークへの影響を避けるために、ACL-ALLOW を使用しています。今後のテストでは、実稼働環境に必要のないトラフィックをブロックする、異なる ACL-DEFAULT を適用する予定です。

ステップ 7 マルチ認証ホスト モードを有効にします。マルチ認証は、基本的には複数ドメイン認証（MDA）のスーパーセットです。MDA では、データ ドメイン内の単一のエンドポイントだけが許可されます。マルチ認証を設定すると、音声ドメイン内では認証された単一の電話が（MDA の場合と同じように）許可されますが、データ ドメイン内では認証できるデータ デバイスの数に制限がありません。

同じ物理アクセスポート上の音声と複数のエンドポイントが許可されます。

authentication host-mode multi-auth

（注） IP 電話の背後で複数のデータ デバイス（仮想デバイスであるかハブに接続されている物理デバイスであるかにかかわらず）を使用すると、アクセス ポートの物理リンクステート認識度が低下する可能性があります。

ステップ 8 次のコマンドを使用して、さまざまな認証方式オプションを有効にします。

次のように、再認証を有効にします。

authentication periodic

次のように、RADIUS セッションタイムアウトを介して再認証を有効にします。

authentication timer reauthenticate server

authentication event fail action next-method

デッドサーバーの場合は、次のようにクリティカル認証 VLAN 方式を設定します。

authentication event server dead action reinitialize vlan *<VLAN_number>*

authentication event server alive action reinitialize

次のように、802.1X と MAB の IOS Flex-Auth 認証を設定します。

authentication order dot1x mab

authentication priority dot1x mab

ステップ 9 次のように、スイッチ ポートで 802.1X ポート制御を有効にします。

authentication port-control auto

authentication violation restrict

ステップ 10 次のように、MAC 認証バイパス（MAB）を有効にします。

mab

ステップ 11 次のように、スイッチポート上で 802.1X を有効にします。

dot1x pae authenticator

ステップ 12 次のように、再送信時間を 10 秒に設定します。

dot1x timeout tx-period *10*

（注） 802.1X tx-period のタイムアウトは 10 秒に設定する必要があります。この値を変更する場合は、その影響を理解したうえで行ってください。

ステップ 13 次のように、PortFast 機能を有効にします。
spanning-tree portfast

EPM ロギングを有効にするコマンド

Cisco ISE の機能について発生する可能性があるトラブルシューティングや記録をサポートするには、スイッチに標準のロギング機能を次のように設定します。

```
epm logging
```

SNMP トラップを有効にするコマンド

次のように、スイッチがこのネットワーク セグメント内の適切な VLAN を経由して、Cisco ISE から SNMP トラップ転送を受信できるようにします。

```
snmp-server community public RO


snmp-server trap-source <VLAN_number>
```

プロファイリング用の SNMP v3 クエリーを有効にするコマンド

SNMP v3 ポーリングが正常に実行され、Cisco ISE プロファイリングサービスがサポートされるように、次のコマンドを使用してスイッチを設定します。その前に、SNMP 設定を Cisco ISE の GUI の [SNMP設定（SNMP Settings）] ウィンドウで設定します。このウィンドウへのナビゲーションパスは、[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）] > [追加 | 編集（Add | Edit）] > [SNMP 設定（SNMP Settings）] ですの順に選択します。

```
Snmp-server user <name> <group> v3 auth md5 <string> priv des <string>


snmp-server group  <group> v3 priv


snmp-server group <group> v3 priv contextvlan-1
```

（注） **snmp-server group** *<group>* **v3 priv context** *vlan-1* コマンドは、コンテキストごとに設定する必要があります。**snmp show context** コマンドでは、すべてのコンテキスト情報がリストされます。

SNMP要求がタイムアウトになり、接続の問題が発生していない場合は、タイムアウト値を増加させることができます。

プロファイラによる収集を可能にするためのMAC通知トラップを有効にするコマンド

次のように、適切な MAC 通知トラップを送信するようスイッチを設定し、Cisco ISE のプロファイラ機能がネットワークエンドポイントで情報を収集できるようにします。

```
mac address-table notification change

mac address-table notification mac-move

snmp trap mac-notification change added

snmp trap mac-notification change removed
```

スイッチ上での RADIUS Idle-timeout の設定

スイッチに RADIUS のアイドルタイムアウトを設定するには、次のコマンドを使用します。

```
Switch(config-if)# authentication timer inactivity
```

ここで、*inactivity*は、クライアントアクティビティが不正と見なされるまでの非アクティブ間隔を秒単位で表したものです。

Cisco ISE では、そのようなセッション非アクティブタイマーを適用する認証ポリシーに対してこのオプションを有効にできます。**[ポリシー（Policy）]**>**[ポリシー要素（Policy Elements）]**>**[結果（Authorization）]**>**[承認（Authorization）]**>**[認証プロファイル（Authorization Profiles）]**を選択しますを選択します。

iOS サプリカントのプロビジョニング用のワイヤレスコントローラの設定

シングル SSID の場合

同じワイヤレスアクセスポイントで、Apple iOS ベースのデバイス（iPhone または iPad）が、ある SSID から別の SSID に切り替えることができるようにするには、**FAST SSID change**機能を有効にするようワイヤレスコントローラを設定します。この機能によって、iOS ベースのデバイスがより迅速に SSID 間の切り替えを行うことができます。

デュアル SSID BYOD の場合

デュアル SSID BYOD をサポートするには、Fast SSID が有効になっている必要があります。ワイヤレスコントローラで Fast SSID Change が有効になっている場合、クライアントは SSID 間を高速で移動できます。高速 SSID が有効になっている場合、クライアント エントリがクリアされず、遅延は適用されません。シスコ ワイヤレス コントローラでの高速 SSID の構成に関する詳細については、『Cisco Wireless Controller Configuration Guide』を参照してください。

ワイヤレスコントローラの構成例

```
WLC (config)# FAST SSID change
```

一部の Apple iOS ベースのデバイスでは、ワイヤレス ネットワークに接続しようとすると、次のエラー メッセージが表示される場合があります。

ワイヤレスネットワークをスキャンできませんでした。（Could not scan for Wireless Networks.）

デバイス認証に影響しないため、このエラー メッセージは無視できます。

モバイルデバイス管理の相互運用のためのワイヤレス LAN コントローラでの ACL の設定

未登録のデバイスおよび証明書プロビジョニングをリダイレクトするために認証ポリシーで使用する ACL をワイヤレスコントローラで設定します。ACL は次の順序にする必要があります。

ステップ 1 サーバーからクライアントへのすべての発信トラフィックを許可します。

ステップ 2 （任意）トラブルシューティングのためにクライアントからサーバーへの ICMP 着信トラフィックを許可します。

ステップ 3 未登録および非準拠のデバイスが MDM エージェントをダウンロードし、コンプライアンスチェックに進むように MDM サーバーへのアクセスを許可します。

ステップ 4 Web ポータルおよびサプリカント用 Cisco ISE、および証明書プロビジョニングフローに対するクライアントからサーバーへのすべての着信トラフィックを許可します。

ステップ 5 名前解決のためにクライアントからサーバーへの着信 DNS トラフィックを許可します。

ステップ 6 IP アドレスのためにクライアントからサーバーへの着信 DHCP トラフィックを許可します。

ステップ 7 Cisco ISE へのリダイレクションのための、クライアントからサーバーへの企業リソースに対するすべての着信トラフィックを（会社のポリシーに応じて）拒否します。

ステップ 8 （任意）残りのトラフィックを許可します。

例

次の例では、未登録のデバイスを BYOD フローにリダイレクトするための ACL を示しています。この例では、Cisco ISE IP アドレスは 10.35.50.165 で、企業のネットワークの IP アドレスは 192.168.0.0 および 172.16.0.0（リダイレクト用）で、MDM サーバーサブネットは 204.8.168.0 です。

図 *1* : 登録されていないデバイスをリダイレクトするための *ACL*

General

Access List Name NSP-ACL

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	150720
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Inbound	7227
3	Permit	0.0.0.0 / 0.0.0.0	204.8.168.0 / 255.255.255.0	Any	Any	Any	Any	Any	17626
4	Permit	0.0.0.0 / 0.0.0.0	10.35.50.165 / 255.255.255.255	Any	Any	Any	Any	Inbound	7505
5	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	2864
6	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DHCP Server	Any	Inbound	0
7	Deny	0.0.0.0 / 0.0.0.0	192.168.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	0
8	Deny	0.0.0.0 / 0.0.0.0	172.16.0.0 / 255.240.0.0	Any	Any	Any	Any	Inbound	4
9	Deny	0.0.0.0 / 0.0.0.0	10.0.0.0 / 255.0.0.0	Any	Any	Any	Any	Inbound	457
10	Deny	0.0.0.0 / 0.0.0.0	173.194.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	1256
11	Deny	0.0.0.0 / 0.0.0.0	171.68.0.0 / 255.252.0.0	Any	Any	Any	Any	Inbound	11310
12	Deny	0.0.0.0 / 0.0.0.0	171.71.181.0 / 255.255.255.0	Any	Any	Any	Any	Any	0
13	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	71819

翻訳について
このドキュメントは、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。