FQDN を使用した ACL の設定

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。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノート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。

FQDN ACL の設定に関する制約事項

FQDN ACL 機能の設定は、IPv4 ワイヤレス セッションでのみサポートされます。

FQDN ACL の設定に関する情報

アクセス コントロール リスト（ACL）が、完全修飾ドメイン名（FQDN）を使用して設定されている場合、宛先ドメイン名に基づいて ACL を適用できます。 宛先のドメイン名はその後、DNS 応答の一部としてクライアントに提供される IP アドレスに解決されます。

ゲスト ユーザは、FQDN ACL 名で構成されるパラメータ マップでネットワーク認証を使用してログインできます。

コントローラに **fqdn-acl-name** AAA 属性を送信するように RADIUS サーバを設定して、アクセス リストを特定のドメインに適用できます。 オペレーティング システムは、パススルー ドメイン リストとそのマッピングを確認し、FQDN を許可します。 FQDN ACL により、クライアントは認証なしで設定されたドメインのみにアクセスできます。

（注） デフォルトでは、IP アクセスリスト名は、パススルードメイン名と同じ名前で設定されます。デフォルト名を上書きするには、グローバル コンフィギュレーション モードで **access-session passthrou-access-group** *access-group-name* **passthrou-domain-list** *domain-list-name* コマンドを使用します。

FQDN ACL の設定方法

FQDN ACL の設定

FQDN ACL を設定するには、次の手順を完了します。

1. IP アクセス リストを作成します。
2. IP ドメイン名リストを作成します。
3. ドメイン名と FQDN ACL をマッピングします。

IP アクセス リストの設定

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `ControllerDevice# 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。

	コマンドまたはアクション	目的
ステップ 2	**ip access-list extended** *name* 例： `ControllerDevice(config)# ip access-list extended ABC`	IP アクセス リストを作成します。
ステップ 3	**permit ip any any** 例： `ControllerDevice(config-ext-nacl)# permit ip any any`	ワイヤレス クライアントに許可されるドメインを指定します。 ドメインはドメイン名リストで指定されます。
ステップ 4	**end** 例： `ControllerDevice(config)# end`	特権 EXEC モードに戻ります。 また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

ドメイン名リストの設定

アクセス ポイントによる DNS スヌーピングが許可されたドメイン名のリストを含むドメイン名リストを設定できます。 DNS ドメイン リスト名の文字列は、拡張アクセス リスト名と一致している必要があります。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `ControllerDevice# 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	**passthrou-domain-list** *name*
	
	例：
	
	`ControllerDevice(config)# passthrou-domain-list abc`
	`ControllerDevice(config-fqdn-acl-domains)#`
		パススルー ドメイン名リストを設定します。

ステップ 3	**match** *word*
	
	例：
	
	`ControllerDevice(config-fqdn-acl-domains)# match play.google.com`
	`ControllerDevice(config-fqdn-acl-domains)# match www.yahoo.com`
		パススルー ドメイン リストを設定します。 クライアントが RADIUS サーバを介して認証される必要なくアクセスの照会が許可される Web サイトのリストを追加します。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `ControllerDevice(config)# end`	特権 EXEC モードに戻ります。 また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

ドメイン名リストの作成（GUI）

ステップ 1 [Configuration] > [Security] > [FQDN] > [Domain Lists] を選択し、[Domain List] ページを開きます。

ステップ 2 次のようにドメイン名を追加します。

a) [Add] をクリックします。 [Add Domain Name List] ページが表示されます。
b) [Domain List Name] テキスト ボックスに、ドメイン リストの名前を入力します。
c) [Domain Name] テキスト ボックスに、リストに追加されるドメインの名前を入力します。
d) [Add Domain] をクリックし、リストにドメインを追加します。
e) リストからドメインを削除するには、ドメインを選択し、[Remove Domain] をクリックします。
f) 設定を保存するには [OK] を、または設定を破棄するには [Cancel] をクリックします。

ドメインが [Domain List] ページに追加されます。

ステップ 3 次のようにドメイン名を編集します。

a) ドメイン リストを選択し、[Modify] をクリックして [Modify Domain Name List] ページを開きます。
b) [Domain Name] テキスト ボックスに、リストに追加されるドメインの名前を入力します。
c) [Add Domain] をクリックし、[OK] をクリックします。
d) リストからドメインを削除するには、ドメイン名をクリックし、[Remove Domain] をクリックします。

ステップ 4 次のようにドメイン名を削除します。

a) ドメインを選択し、[Remove] をクリックします。 ドメインがドメイン名リストから削除されます。
b) 設定を保存するには [OK] を、または設定を破棄するには [Cancel] をクリックします。

ドメイン名と FQDN ACL のマッピング

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `ControllerDevice# 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	**access-session passthrou-access-group** *access-group-name* **passthrou-domain-list** *domain-list-name* 例： `ControllerDevice(config)# access-session passthrou-access-group abc passthrou-domain-list abc`	ドメイン名リストと FQDN ACL AAA 属性名をマッピングします。 中央 Web 認証を設定する場合、このコマンドを使用します。

ステップ 3	**parameter-map type webauth** *domain-list-name* and **login-auth-bypass fqdn-acl-name** *acl-name* **domain-name** *domain-name*
	
	例：
	`ControllerDevice(config)# parameter-map type webauth abc`
	`ControllerDevice(config-params-parameter-map)# login-auth-bypass fqdn-acl-name abc domain-name abc`
		ドメイン名リストと FQDN ACL 名をマッピングします。 コントローラでローカル認証を設定する場合、このコマンドを使用します。
		
		RADIUS サーバは、認証されたユーザ プロファイルの一部として FQDN ACL 名を返すように設定できます。FQDN ACL がコントローラで定義される場合、コントローラは FQDN ACL をユーザに動的に適用します。

ドメイン名と FQDN ACL のマッピング（GUI）

ステップ 1 [Configuration] > [Security] > [FQDN] > [Parameter Mapping] を選択して、[Parameter Mapping] ページを開きます。

ステップ 2 次のように、パラメータ マップにドメイン リストとアクセス リストを追加します。

a) [Domain List Name] ドロップダウン リストから、ドメイン リスト名を選択します。
b) [Access List] ドロップダウン リストから、アクセス リスト名を選択します。
c) [Global] を選択します。
d) パラメータ マップ リストで、パラメータ マップを選択します。
e) 設定を保存するには [OK] を、または設定を破棄するには [Cancel] をクリックします。
ドメイン名リストと FQDN ACL が [Parameter Mapping] ページに表示されます。

ステップ 3 次のように、ドメイン リストとアクセス リストを変更します。

a) ドメイン リストを選択し、[Modify] をクリックして [Modify Parameter Mapping] ページを開きます。
b) [Domain List Name] ドロップダウン リストから、ドメイン リスト名を選択します。
c) [Access List] ドロップダウン リストから、アクセス リスト名を選択します。
d) [Global] を選択してマッピングをグローバルにイネーブルにするか、Web 認証用のパラメータ マップを選択します。
グローバルおよびパラメータ マップ オプションを一緒にまたは別々に選択できます。
e) [Parameter map] テキスト ボックスで、Web 認証パラメータ マップを 1 つ選択します。
f) FQDN 設定を適用するには [OK] を、または設定を破棄するには [Cancel] をクリックします。
ドメイン名リストと FQDN ACL が [Parameter Mapping] ページに表示されます。

ステップ 4 次のようにドメイン リストを削除します。

a) ドメイン名リストを選択し、[Remove] をクリックします。 ドメイン名リストが削除されます。
b) 設定を正常に適用するには [OK] を、または設定を破棄するには [Cancel] をクリックします。

FQDN ACL のモニタリング

次のコマンドを使用して FQDN ACL を監視できます。

コマンド	目的
show access-session interface *interface-name* **details**	インターフェイスに設定された FQDN ACL 情報を表示します。
show access-session fqdn fqdn-maps	ドメイン名リストにマッピングされた FQDN ACL を表示します。
show access-session fqdn list-domain *domain-name*	ドメイン名を表示します。
show access-session fqdn passthru-domain-list	設定されているドメインを表示します。

例：FQDN ACL の設定

次に、IP アクセス リストを作成する例を示します。

```
ControllerDevice# config terminal
ControllerDevice(config)# ip access-list extended abc
ControllerDevice(config-ext-nacl)# permit ip any any
ControllerDevice(config-ext-nacl)# end
ControllerDevice# show ip access-list abc
```

次に、ドメイン名のリストを設定する例を示します。

```
ControllerDevice# config terminal
ControllerDevice(config)# passthrou-domain-list abc
ControllerDevice(config-fqdn-acl-domains)# match play.google.com
ControllerDevice(config-fqdn-acl-domains)# end
ControllerDevice# show access-session fqdn fqdn-maps
```

次に、中央集中型Web認証を使用してドメイン名とFQDN ACLをマッピングする例を示します。

```
ControllerDevice# config terminal
ControllerDevice(config)# access-session passthrou-access-group abc passthrou-domain-list
abc
ControllerDevice(config)# end
ControllerDevice# show access-session interface vlan 20
```

次に、ローカル認証を使用してドメイン名と FQDN ACL をマッピングする例を示します。

```
ControllerDevice# config terminal
ControllerDevice(config)# parameter-map type webauth abc
ControllerDevice(config-params-parameter-map)# login-auth-bypass fqdn-acl-name abc domain-name
 abc
ControllerDevice(config-params-parameter-map)# end
ControllerDevice# show access-session fqdn fqdn-maps
```

FQDN ACL の設定に関する追加情報

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	セキュリティ コマンド リファレンス ガイド、*Cisco IOS XE* リリース *3E*（*Cisco WLC 5700* シリーズ）

標準および RFC

標準/RFC	Title
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	Link
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。 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。 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。	http://www.cisco.com/support

FQDN ACL の設定に関する機能履歴と情報

リリース	機能情報
Cisco IOS XE 3E	この機能が導入されました。

セキュリティ コンフィギュレーション ガイド、Cisco IOS XE リリース 3E（Cisco WLC 5700 シリーズ）