Cisco Prime Infrastructure 3.0
リファレンス ガイド

2015 年 8 月

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/

Text Part Number:

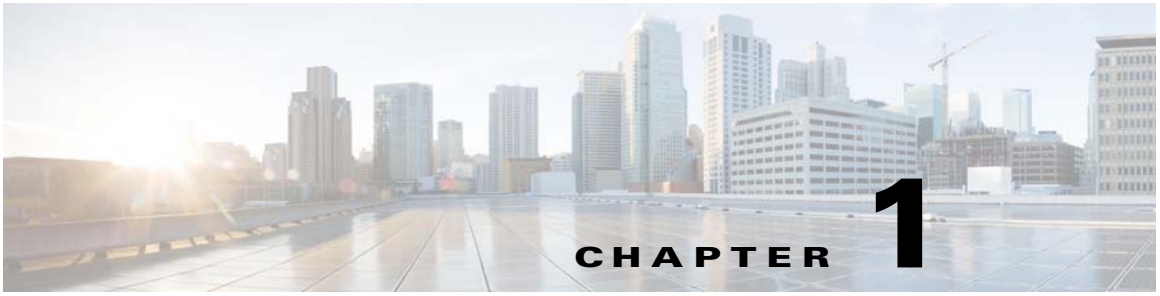
【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ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。

Cisco Prime Infrastructure 3.0 リファレンス ガイド

CONTENTS



[Monitor] ページのフィールド リファレンス

ここでは、Cisco Prime Infrastructure リリース 3.0 の [Monitor] タブにあるフィールドについて説明します。

ネットワーク デバイス

次に、フィールドについて説明します。

[Monitor] > [Switches] > [Search]

次の表で、スイッチに高度な検索を実行した場合の各フィールドについて説明します。

表 1-1　[Search Switches] フィールド

フィールド	オプション
Search for Switches by	[All Switches]、[IP Address]、または [Switch Name] を選択します。ワイルドカード (*) を使用できます。例えば、[IP Address] を選択して 172* を入力した場合、Prime Infrastructure は IP アドレスが 172 で始まるすべてのスイッチを返します。
Items per page	ページあたりに返すスイッチの数を選択します。

[Monitor] > [Switches] > [View]

次の表で、スイッチのサマリが表示されるページの各フィールドについて説明します。

表 1-2　スイッチの表示

フィールド	説明
IP Address	スイッチに割り当てられている IP アドレス。リスト項目をクリックするとアクセス ポイントの詳細が表示されます。
Device Name	スイッチ名。
Device Type	スイッチのタイプ。

表 1-2　スイッチの表示（続き）

フィールド	説明
Reachability Status	スイッチが到達可能な場合は [OK] が表示され、スイッチが到達不能な場合は [Unreachable] が表示されます。
Endpoint Count	スイッチ上のエンドポイントの数。

[Monitor] > [Switches] > [IP Address]

次の表で、スイッチのサマリ ページに表示されるサマリ情報について説明します。

表 1-3　スイッチの要約情報の表示

General	
IP Address	スイッチの IP アドレス。
Device Name	スイッチ名。
Device Type	スイッチの種類。
Up Time	最後にリブートしてからの時間。
System Time	スイッチ上の時刻。
Reachability Status	有効な値は次のとおりです。 • Reachable • Unreachable
Location	スイッチの場所。
Contact	スイッチの担当者名。
Cisco Identity Capable	スイッチがアイデンティティ対応かどうかを示します。
Location Capable	スイッチがロケーション情報を保存できるかどうかを示します。
CPU Utilization	指定した期間の最大、平均、および最小 CPU 使用率のグラフが表示されます。
Unique Device Identifier (UDI)	
Name	製品の種類。
Description	UDI の説明。
Product ID	注文可能な製品 ID。
Version ID	製品 ID のバージョン。
Serial Number	一意の製品シリアル番号。
Name	
Software Version	現在スイッチで動作しているソフトウェアのバージョン。
Model No.	スイッチのモデル番号。
Port Summary	
Number of Ports Up	スイッチでアップ状態のポートの数。

表 1-3　スイッチの要約情報の表示（続き）

Number of Ports Down	スイッチでダウン状態のポートの数。
Memory Utilization	指定した期間の最大、平均、および最小メモリ使用率のグラフが表示されます。

[Monitor] > [Switches] > [Memory]

次の表で、スイッチのメモリ情報について説明します。

表 1-4　スイッチのメモリ情報の表示

Memory Pool	
Type	メモリのタイプ。
Name	メモリ プールに割り当てられた名前。
Used (MB)	使用中のメモリ量(MB 単位)。
Free (MB)	使用可能なメモリ量(MB 単位)。

[Monitor] > [Switches] > [Environment]

次の表で、スイッチの環境情報について説明します。

表 1-5　スイッチの環境情報の表示

Power Supply	
Model Name	電源のモデル名。
Description	電源の説明。
Operational Status	関連付けられている電源のステータス。 • 緑:電源は動作可能です。 • 赤:電源は動作不能です。
Manufacturer Name	電源のメーカー名。
Free	空き電源スロット。
Vendor Equipment Type	ベンダー製機器タイプの説明。
Fans	
Name	ファンの名前。
Description	ファンの説明。
Operational Status	ファンのステータス。 • 緑:ファンは動作可能です。 • 赤:ファンは動作不能です。
Vendor Equipment Type	ベンダー製機器タイプの説明。
Serial Number	ファンのシリアル番号。

[Monitor] > [Switches] > [Modules]

次の表で、スイッチのモジュール情報について説明します。

表 1-6　スイッチ モジュール情報の表示

Modules	
Product Name	モジュールの名前。
Physical Location	モジュールが格納されている場所。
Number of Ports	モジュールがサポートするポートの数。
Operational State	モジュールの動作ステータス。
Equipment Type	機器の種類。
Inline Power Capable	モジュールにインライン パワー機能があるかどうかを示します。

[Monitor] > [Switches] > [VLANs]

次の表で、スイッチの VLAN 情報について説明します。

表 1-7　スイッチの VLAN 情報の表示

VLANs	
VLAN ID	VLAN の ID。
VLAN Name	VLAN の名前。
VLAN Type	VLAN の種類。

[Monitor] > [Switches] > [VTP]

次の表で、スイッチの VTP 情報について説明します。

表 1-8　スイッチの VTP 情報の表示

VTP	
VTP Domain Name	VTP ドメインの名前。
VTP Version	使用している VTP のバージョン。
VTP Mode	VTP モード。 • [Client] • [Server] • [Transparent]:VTP メッセージを生成またはリッスンしませんが、メッセージを転送します。 • [Off]:VTP メッセージを生成、リッスン、転送しません。
Pruning Enabled	VTP プルーニングが有効かどうかを示します。

[Monitor] > [Switches] > [Physical Ports]

次の表で、スイッチの物理ポート情報について説明します。

表 1-9　スイッチの物理ポート情報の表示

Physical Ports	
Port Name	物理ポートの名前。
Port Description	物理ポートの説明。
Residing Module	物理ポートがあるモジュール。
Vendor Equipment Type	ベンダー製機器タイプの説明。

[Monitor] > [Switches] > [Sensors]

次の表で、スイッチのセンサー情報について説明します。

表 1-10　スイッチのセンサー情報の表示

Sensor	
Sensor Name	センサーの名前。
Sensor Description	センサーの説明
Type	センサーの種類。
Vendor Sensor Type	ベンダー製センサーの種類の説明。
Equipment Name	機器の名前。
Precision	範囲が 1 ～ 9 の場合、精度は、センサー値の固定小数点数値の小数点以下の桁数です。範囲が -8 ～ -1 の場合、センサーの精度は、センサー値の固定小数点数値の正確な桁数です。
Status	センサーの動作ステータス。

[Monitor] > [Switches] > [Spanning Tree]

次の表で、スパニング ツリー情報について説明します。

表 1-11　スイッチのスパニング ツリー情報の表示

Spanning Tree	
STP Instance ID	STP の ID。スパニング ツリーの詳細情報を表示するには、[STP Instance ID] をクリックします。
VLAN ID	VLAN の ID。
Root Path Cost	パスのルート コスト。
Designated Root	転送ポート。
Bridge Priority	ブリッジのプライオリティ。
Root Bridge Priority	ルート ブリッジのプライオリティ番号。

表 1-11　スイッチのスパニング ツリー情報の表示（続き）

Max Age (sec)	最大経過時間の STP タイマー値(秒単位)。
Hello Interval (sec)	STP タイマー値(秒単位)。

[Monitor] > [Switches] > [Spanning Tree] > [STP instance ID]

次の表で、スパニング ツリーの詳細情報のページにあるフィールドについて説明します。

表 1-12　スパニング ツリーの詳細の表示

Spanning Tree	
STP Port	STP ポートの名前。
Port Role	ポートのロール。
Port Priority	ポートのプライオリティ番号。
Path Cost	パスのコスト。
Port State	ポートの状態。
Port Type	ポートの種類。

[Monitor] > [Switches] > [Stacks]

次の表で、スイッチ スタック情報のページにあるフィールドについて説明します。

表 1-13　スイッチのスタック情報の表示

Stacks	
MAC Address	スタックの MAC アドレス。
Role	スタックの役割。 • [Master]:スタック マスター • [Member]:スタックのアクティブ メンバー • [Not Member]:非アクティブ スタック メンバー
Switch Priority	スイッチのプライオリティ番号。
State	スタックの現在の状態。
Software Version	スイッチで動作しているソフトウェア イメージ。

[Monitor] > [Switches] > [Interfaces] > [Ethernet Interfaces]

次の表で、スイッチのイーサネット インターフェイスのページにあるフィールドについて説明します。

表 1-14　スイッチのイーサネット インターフェイスの表示

Name	イーサネット インターフェイスの名前。詳細情報を表示するには、イーサネット インターフェイスの名前をクリックします。
MAC Address	イーサネット インターフェイスの MAC アドレス。
Speed (Mbps)	イーサネット インターフェイスの現在の帯域幅の推測値(bps 単位)。
Operational Status	イーサネット インターフェイスの現在の動作状態。
MTU	インターフェイスで送受信できる最大のパケット サイズ。
Desired VLAN Mode	VLAN モード。
Access VLAN	ポートが設定されている VLAN。

[Monitor] > [Switches] > [Interfaces] > [Ethernet Interface Name]

次の表で、スイッチのイーサネット インターフェイスの詳細情報のページにあるフィールドについて説明します。

表 1-15　スイッチのイーサネット インターフェイスの詳細の表示

Ethernet Interfaces	
Name	イーサネット インターフェイスの名前。
Admin Status	インターフェイスの管理ステータス。
Duplex Mode	インターフェイスで設定されているデュプレックス モード。
VLAN Switch Port	
Operational VLAN Mode	VLAN スイッチ ポートの動作モードを示します(アクセス ポートまたはトランク ポート)。
Desired VLAN Mode	VLAN モード(truck、access、dynamic、または desirable)。
Access VLAN	ポートが設定されている VLAN。
Operational Truck Encapsulation	トランクのカプセル化(*802.1Q* または *none*)。
VLAN Trunk	
Native VLAN	トランク スイッチ ポートのタグなしの VLAN。
Prune Eligible	トランク ポート上の VLAN をプルーニングできるかどうかを示します。
Allows VLANs	トランク ポート上の許可される VLAN のリスト。
Desired Trunking Encapsulation	トランク カプセル化
Trunking Encapsulation Negotiation	インターフェイスがネイバー インターフェイスとネゴシエーションを行い、近接インターフェイスの設定および機能に応じて、ISL トランク(優先)または 802.1Q トランクになるよう指定します。

[Monitor] > [Switches] > [Interfaces] > [IP Interface]

次の表で、スイッチの IP インターフェイスのページにあるフィールドについて説明します。

表 1-16　スイッチの IP インターフェイスの表示

Interface	インターフェイスの名前。
IP Address	インターフェイスの IP アドレス。
Address Type	アドレス タイプ（IPv4 または IPv6）。

[Monitor] > [Switches] > [Interfaces] > [VLAN Interface]

次の表で、スイッチの VLAN インターフェイスのページにあるフィールドについて説明します。

表 1-17　スイッチの VLAN インターフェイスの表示

Port Name	VLAN ポートの名前。
VLAN ID	VLAN ポートの ID。
Operational Status	VLAN インターフェイスの現在の動作状態。
Admin Status	VLAN インターフェイスの現在の管理状態。
Port Type	VLAN ポートの種類。
Maximum Speed (Mbps)	VLAN インターフェイスのサポートされる最大速度。
MTU	VLAN インターフェイスで送受信できる最大のパケット サイズ。

[Monitor] > [Switches] > [Interfaces] > [EtherChannel Interface]

次の表で、スイッチの EtherChannel インターフェイスのページにあるフィールドについて説明します。

表 1-18　EtherChannel インターフェイスの表示

Name	EtherChannel インターフェイスの名前。
Channel Group ID	EtherChannel の数値 ID。
Control Method	EtherChannel を管理するためのプロトコル（LACP または TAgP）。
Actor Admin Key	チャネル ID。
Number of (LAG) Members	設定されているポート数。

[Monitor] > [Switches] > [Client]

次の表で、スイッチ クライアントのページにあるフィールドについて説明します。

表 1-19　現在関連付けられているクライアントの表示

IP Address	クライアントの IP アドレス。
MAC Address	クライアントの MAC アドレス。
User Name	クライアントのユーザ名。
Vendor Name	クライアントのベンダー名。
Map Location	クライアントの場所。
VLAN	クライアントが設定されている VLAN。
Interface	クライアントが設定されているインターフェイス。
Association Time	クライアント アソシエーションのタイムスタンプ。
Authorization Profile Name	格納されている認可プロファイル名。

[Monitor] > [Wireless Technologies] > [Access Point Radios]

表 1-20 で、[Monitor] > [Wireless Technologies] > [Access Point Radios] の各フィールドについて説明します。

表 1-20　[Access Point Search Results] フィールド

フィールド	説明
AP Name	アクセス ポイントに割り当てられた名前。
Ethernet MAC	AP イーサネットの MAC アドレス。
IP Address	アクセス ポイントのローカル IP アドレス。
Radio	不正アクセス ポイントのプロトコルは、802.11a、802.11b、または 802.11g です。 リスト項目をクリックするとアクセス ポイントの無線の詳細が表示されます。
Map Location	リスト項目をクリックすると、リストで示された場所に移動します。
Controller	リスト項目をクリックすると、コントローラに関するグラフィックと情報が表示されます。
Client Count	現在コントローラにアソシエートされているクライアントの合計数が表示されます。
Admin Status	アクセス ポイントの管理状態が、有効または無効で表示されます。
AP Mode	アクセス ポイントの動作モードが表示されます。

表 1-20　[Access Point Search Results] フィールド（続き）

フィールド	説明
Oper Status	Cisco WLAN Solution デバイスの動作ステータス（Up または Down）が表示されます。[Admin Status] が disabled の場合、動作ステータスはダウンとラベル付けされ、アラームはありません。
Alarm Status	アラームのカラー コードは、次のとおりです。 • Clear-No アラーム • Red-Critical アラーム • Orange-Major アラーム • Yellow-Minor アラーム

[Monitor] > [Wireless Technologies] > [Access Point Radios] > [Edit View]

表 1-21 で、[Monitor] > [Wireless Technologies] > [Access Point Radios] > [Edit View] の各フィールドについて説明します。

表 1-21　[Edit View Search Results] フィールド

フィールド	説明
AP Type	アクセス ポイントのタイプ（[Unified] または [Autonomous]）を表示します。
Antenna Azim. Angle	アンテナの水平方向の角度を表示します。
Antenna Diversity	アンテナの多様性が有効か無効かを表示します。アンテナ ダイバーシティは、適切なアンテナを選択するためにアクセス ポイントが 2 つの統合アンテナ ポートから無線信号をサンプリングすることをいいます。
Antenna Elev. Angle	アンテナの垂直方向の角度を表示します。
Antenna Gain	無線ネットワーク アダプタに接続される指向性アンテナのピーク ゲイン（dBi）、および全方向性アンテナの平均ゲイン（dBi）。ゲインは 0.5dBi の倍数で表します。整数値 4 は、4 X 0.5 = 2dBi のゲインであることを意味します。
Antenna Mode	全方向、指向性、または該当なしなどのアンテナ モードを表示します。
Antenna Name	アンテナの名前またはタイプを表示します。
Audit Status	次の監査ステータスのいずれかを表示します。 • [Mismatch]：最後の監査時に Prime Infrastructure とコントローラ間に設定上の相違が検出されました。 • [Identical]：最後の監査時に設定上の相違は検出されませんした。 • [Not Available]：監査ステータスは利用できません。
Base Radio MAC	ベース無線の MAC アドレスを表示します。
Bridge Group Name	アクセス ポイントのグループ化に使用するブリッジ グループの名前を表示します（該当する場合）。
CDP Neighbors	直接接続されているすべてのシスコ デバイスを表示します。
Channel Control	チャネル制御が自動かカスタムかを表示します。
Channel Number	シスコの無線をブロードキャストしているチャネルを表示します。

表 1-21　[Edit View Search Results] フィールド（続き）

フィールド	説明
Channel Width	この無線のチャネル帯域幅を表示します。[Channel Width] フィールドは、11n AP のみでサポートされます。その他の AP については「N/A」を表示します。
Controller Port	コントローラ ポートの数を表示します。
Google Earth Location	Google Earth の場所情報が割り当てられているかどうかを表示し、その場所を表示します。
Location	アクセス ポイントの物理的な場所を表示します。
Node Hops	アクセス ポイント間のホップの数を表示します。
OfficeExtend AP	OfficeExtend アクセスが有効かどうかを示します。無効の場合、アクセス ポイントはリモートで配置されており、セキュリティ リスクが高まります。
PoE Status	アクセス ポイントの Power over Ethernet のステータスを表示します。可能な値は次のとおりです。 • [Low]：アクセス ポイントがイーサネットから低電力を取得します。 • [Lower than 15.4 volts]：アクセス ポイントがイーサネットから 15.4 ボルト未満の電力を取得します。 • [Lower than 16.8 volts]：アクセス ポイントがイーサネットから 16.8 ボルト未満の電力を取得します。 • [Normal]：電力はアクセス ポイントの動作に十分な高さです。 • [Not Applicable]：イーサネットは電力源ではありません。
Primary Controller	このアクセス ポイントのプライマリ コントローラの名前を表示します。
Radio MAC	無線の MAC アドレスを入力します。
Reg. Domain Supported	規制ドメインをサポートしているかどうかを表示します。
Serial Number	アクセス ポイントのシリアル番号を入力します。
Slot	スロット番号を表示します。
Tx Power Control	送信電力制御が自動かカスタムかを表示します。
Tx Power Level	送信電力レベルを設定します。
Up Time	アクセス ポイントがアップしていた時間を、日、時間、分、および秒の単位で表示します。
WLAN Override Names	WLAN の上書きプロファイル名を入力します。
WLAN Override	WLAN の上書きが有効か無効かを表示します。

[Monitor] > [Wireless Technologies] > [Access Point Radios] > [Load]

表 1-22 で、[Monitor] > [Wireless Technologies] > [Access Point Radios] > [Load] の各フィールドについて説明します。

表 1-22　[Traffic Load] ページのフィールド

フィールド	説明
AP Name	アクセス ポイントの名前を表示します。
Radio	不正アクセス ポイントのプロトコルを表示します。802.11a、802.11b、または 802.11g のいずれかです。このアクセス ポイントのオンデマンド統計情報を表示するには、無線をクリックします。
Attached Client Count	接続されているクライアントの数を表示します(実際の数としきい値)。
Channel Utilization	802.11a RF の使用率のしきい値を 0 ～ 100 % の範囲で表示します(実際の割合としきい値)。
Receive Utilization	802.11a または 802.11b/g RF の受信使用率のしきい値を 0 ～ 100 % の範囲で表示します。
Transmit Utilization	802.11a または 802.11b/g RF の送信使用率のしきい値を 0 ～ 100 % の範囲で表示します。
Status	クライアント接続のステータスを表示します。

[Monitor] > [Wireless Technologies] > [Access Point Radios] > [Dynamic Power Control]

表 1-23 で、[Monitor] > [Wireless Technologies] > [Access Point Radios] > [Dynamic Power Control] の各フィールドについて説明します。

表 1-23　[Dynamic Power Control] ページのフィールド

フィールド	説明
AP Name	AP の名前を表示します。
Radio	不正アクセス ポイントのプロトコルを表示します。802.11a、802.11b、または 802.11g のいずれかです。このアクセス ポイントのオンデマンド統計情報を表示するには、無線をクリックします。

表 1-23　[Dynamic Power Control] ページのフィールド（続き）

フィールド	説明
Current Power Level	送信電力テーブルから取得した動作送信電力レベルが表示されます。 電力レベルおよび使用可能なチャネルは国コード設定によって定義されており、国別に規制されています。 AP の送信電力レベルは次のとおりです。 • 1:国コード設定ごとに許可された最大電力 • 2:50 % の電力 • 3:25 % の電力 • 4:6.25 ～ 12.5 % の電力 • 5:0.195 ～ 6.25 % の電力
Power Assignment Mode	動的な送信電力の割り当てを表示します。次の 3 つのモードを使用できます。 • [Automatic]:送信電力は、この操作を許可するすべての Cisco 1000 シリーズの Lightweight アクセス ポイントで定期的に更新されます。 • [On Demand]:送信電力は、[Assign Now] ボタンがオンの場合に更新されます。 • [Fixed]:動的な送信電力の割り当ては行われず、値はグローバル デフォルトに設定されます。デフォルトは Automatic です。

[Monitor] > [Wireless Technologies] > [Access Point Radios] > [Voice TSM Table]

表 1-24 で、[Monitor] > [Wireless Technologies] > [Access Point Radios] > [Voice TSM Table] の各フィールドについて説明します。

表 1-24　[Voice Traffic Stream Metrics Table] ページのフィールド

フィールド	説明
Time	アクセス ポイントから統計情報が収集された時刻。
Client MAC	クライアントの MAC アドレス。これには、過去 90 秒の間隔中に評価されたクライアントのリストが表示されます。クライアントとしては、VoIP 電話、ラップトップ、PDA などがあり、測定値を収集しているアクセス ポイントに接続されたすべてのクライアントを示します。
QoS	WLAN に影響を与える可能性のある QoS 値（パケット遅延、パケット ジッタ、パケット損失、ローミング時間）がモニタされます。アクセス ポイントおよびクライアントでメトリックを測定し、アクセス ポイントで計測結果を収集してこれらをコントローラに送信します。アクセス ポイントでは、90 秒ごとにコントローラのトラフィック ストリーム メトリック情報を更新し、一度に 10 分間分のデータが格納されます。
% PLR (Downlink)	90 秒の間隔中にダウンリンク（アクセス ポイントからクライアントへ向かう方向）で失われたパケットの割合。
% PLR (Uplink)	90 秒の間隔中にアップリンク（クライアントからアクセス ポイントへ向かう方向）で失われたパケットの割合。

表 1-24　[Voice Traffic Stream Metrics Table] ページのフィールド（続き）

フィールド	説明
Avg Queuing Delay (ms) (Downlink)	ダウンリンクの平均キューイング遅延(ミリ秒単位)。パケット キューイング遅延の平均は、音声キューを横断する音声パケットの平均遅延です。パケット キュー遅延は、パケットが送信のためにキューに入れられた時点から、パケットが正常に送信される時点まで測定されます。これには、必要に応じて再試行時間が含まれます。
Avg Queuing Delay (ms) (Uplink)	アップリンクの平均キューイング遅延(ミリ秒単位)。パケット キューイング遅延の平均は、音声キューを横断する音声パケットの平均遅延です。パケット キュー遅延は、パケットが送信のためにキューに入れられた時点から、パケットが正常に送信される時点まで測定されます。これには、必要に応じて再試行時間が含まれます。
% Packets > 40 ms Queuing Delay	40 ms を超えるキューイング遅延パケットのパーセンテージ。
% Packets > 20 ms Queuing Delay	20 ms を超えるキューイング遅延パケットのパーセンテージ。
Roaming Delay	ローミング遅延(ミリ秒単位)。クライアントによって測定されるローミング遅延は、古いアクセス ポイントから最後のパケットを受信した時点から、ローミングが正常に行われた後で新しいアクセス ポイントから最初のパケットを受信した時点まで測定されます。

[Monitor] > [Wireless Technologies] > [Access Point Radios] > [Voice TSM Reports]

表 1-25 で、[Monitor] > [Wireless Technologies] > [Access Point Radios] > [Voice TSM Reports] の各フィールドについて説明します。

表 1-25　[Voice Traffic Stream Metrics Table Reports] ページのフィールド

フィールド	説明
Average Queuing Delay (ms)	平均キューイング遅延(ミリ秒単位)。パケット キューイング遅延の平均は、音声キューを横断する音声パケットの平均遅延です。パケット キュー遅延は、パケットが送信のためにキューに入れられた時点から、パケットが正常に送信される時点まで測定されます。これには、必要に応じて再試行時間が含まれます。
% Packet with less than 10 ms delay	遅延が 10 ミリ秒未満のパケットのパーセンテージ。
% Packet with more than 10 < 20 ms delay	遅延が 10 ミリ秒よりも大きく 20 ミリ秒未満のパケットのパーセンテージ。
% Packet with more than 20 < 40 ms delay	遅延が 20 ミリ秒よりも大きく 40 ミリ秒未満のパケットのパーセンテージ。
% Packet with more than 40 ms delay	遅延が 40 ミリ秒よりも大きいパケットのパーセンテージ。
Packet Loss Ratio	失われたパケットの割合。
Total Packet Count	パケットの総数。

表 1-25　[Voice Traffic Stream Metrics Table Reports] ページのフィールド（続き）

フィールド	説明
Roaming Count	この 90 秒間のメトリック ページでローミング ネゴシエーションのために交換されたパケットの数。
Roaming Delay	ローミング遅延（ミリ秒単位）。

[Monitor] > [Wireless Technologies] > [Access Point Radios] > [General]

表 1-26 で、[Monitor] > [Wireless Technologies] > [Access Point Radios] > [General] の Lightweight アクセス ポイントの各フィールドについて説明します。

表 1-26　Lightweight アクセス ポイントの [General] タブのフィールド

フィールド	説明
General	
AP Name	AP のオペレータ定義の名前。
AP IP address、Ethernet MAC address、および Base Radio MAC address	IP アドレス、イーサネット MAC アドレス、および無線 MAC アドレス。
Country Code	サポートされる国コード。1 台のコントローラで最大 20 の国をサポートできます。 運用する国向けに設計されていない場合、アクセス ポイントは正しく動作しない可能性があります。製品ごとの完全な国コードのリストについては、http://www.cisco.com/en/US/docs/wireless/wcs/4.0/configuration/guide/wcscod.html を参照してください。
Link Latency Settings	リンク遅延設定。次のリンク遅延が使用できます。 • [Current Link Latency]：アクセス ポイントからコントローラ、およびその逆のハートビート パケットの秒単位での現在のラウンドトリップ時間。 • [Minimum Link Latency]：リンク遅延を有効にしたか、リセットした場合のアクセス ポイントからコントローラ、およびその逆のハートビート パケットの秒単位での最小ラウンドトリップ時間。 • [Maximum Link Latency]：リンク遅延を有効にしたか、リセットした場合のアクセス ポイントからコントローラ、およびその逆のハートビート パケットの秒単位での最大ラウンドトリップ時間。
LWAPP/CAPWAP Uptime	LWAPP/CAPWAP 接続がアクティブになっていた時間が表示されます。
LWAPP/CAPWAP Join Taken Time	LWAPP/CAPWAP 接続が参加していた時間が表示されます。
Admin Status	アクセス ポイントの管理状態が、有効または無効で表示されます。

表 1-26　Lightweight アクセス ポイントの [General] タブのフィールド（続き）

フィールド	説明
AP Mode	
Local	デフォルト モード。設定したチャネルをスキャンしてノイズと不正を探す間、データ クライアントにサービスが提供されます。アクセス ポイントは 50 ミリ秒間、チャネルの不正をリッスンします。Auto RF 設定の下で指定された期間の間、各チャネルを巡回します。 Cisco Adaptive wIPS 機能にローカルまたは FlexConnect のアクセス ポイントを設定するには、[Local] または [FlexConnect] を選択し、[Enhanced wIPS Engine Enabled] チェックボックスをオンにします。
Monitor	無線受信専用モード。アクセス ポイントは、設定されたすべてのチャネルを 12 秒ごとにスキャンします。このように設定されたアクセス ポイントでは、認証解除のパケットだけが無線で送信されます。モニタ モード アクセス ポイントは、不正アクセス ポイントにクライアントとして接続できます。 Cisco Adaptive wIPS 機能にアクセス ポイントを設定するには、[Monitor] を選択します。[Enhanced wIPS Engine Enabled] チェックボックスをオンにして、[Monitor Mode Optimization] ドロップダウン リストから [wIPS] を選択します。 アクセス ポイントで wIPS モードを有効にする前に、アクセス ポイントの無線を無効にする必要があります。アクセス ポイントの無線を無効にしないと、エラー メッセージが表示されます。 wIPS をアクセス ポイントで有効にした後で無線を一度再有効化しています。
Rogue Detector	アクセス ポイントの無線がオフに切り替わり、アクセス ポイントは有線トラフィックだけをリッスンします。このモードで動作するコントローラは、不正アクセス ポイントをモニタします。コントローラはすべての不正アクセス ポイントとクライアントの MAC アドレスのリストを不正検出器に送信して、不正検出器がこの情報を WLC に転送します。MAC アドレスの一覧が、WLC アクセス ポイントがネットワーク上で取得した内容と比較されます。MAC アドレスが一致する場合は、どの不正アクセス ポイントが有線ネットワークに接続されるかを判別できます。
Sniffer	アクセス ポイントは特定チャネル上のすべてのパケットを取得して、AiroPeek を実行するリモート マシンへ転送します。これらのパケットには、タイムスタンプ、信号強度、パケット サイズなどの情報が含まれます。この機能は、データ パケットのデコードをサポートする、サードパーティ製のネットワーク分析ソフトウェアである AiroPeek を実行する場合のみ有効にできます。
FlexConnect	FlexConnect アクセス ポイントは、コントローラへの接続を失ったとき、クライアント データ トラフィックをローカルにスイッチングし、クライアント認証をローカルで実行できます。 OfficeExtend アクセス ポイントを設定するには、[FlexConnect] を選択する必要があります。FlexConnect モードでは、設定オプションに OfficeExtend AP を有効にして Least Latency Controller を接続できるようにするオプションが表示されます。

表 1-26　Lightweight アクセス ポイントの [General] タブのフィールド（続き）

フィールド	説明
Bridge	これは、Autonomous アクセス ポイントが無線クライアントのように機能して、Lightweight アクセス ポイントに接続する特殊なモードです。AP モードが [Bridge] に設定され、アクセス ポイントがブリッジ対応である場合、ブリッジとその有線クライアントは、Prime Infrastructure にクライアントとしてリストされます。
Spectrum Expert	このモードでは、CleanAir 対応のアクセス ポイントを、すべてのモニタ対象チャネル上の干渉源検出のために広範囲に使用できます。IDS スキャンや Wi-Fi などのその他の機能はすべて一時停止されます。
Enhanced wIPS Engine	[Enabled] または [Disabled] のいずれかが設定され、Cisco Adaptive wIPS 機能を使用したセキュリティ攻撃のモニタが可能となります。
Operational Status	[Registered] または [Not Registered] のいずれかとなり、コントローラで決定されます。
Registered Controller	アクセス ポイントが登録されているコントローラ。登録済みのコントローラの詳細を表示します。
Primary Controller	このアクセス ポイントのプライマリ コントローラの名前。
Port Number	アクセス ポイントのプライマリ コントローラの SNMP 名。アクセス ポイントは、すべてのネットワーク操作について、ハードウェア リセットが発生した場合、このコントローラに最初にアソシエートしようとします。
AP Uptime	アクセス ポイントがアクティブで送受信できる状態になっている時間を表示します。
Map Location	アクセス ポイントのカスタマー定義の場所名。クリックするとマップ上で実際の場所が表示されます。詳細については、[Monitor] > [Access Points] > [name] > [Map Location] を選択します。
Google Earth Location	Google Earth の場所が割り当てられているかどうかを示します。
Location	アクセス ポイントが配置されている物理的な場所（または Unassigned）。
Statistics Timer	このカウンタは、アクセス ポイントがその DOT11 統計情報をコントローラに送信する時間を秒単位で設定します。
PoE Status	アクセス ポイントの Power over Ethernet のステータス。次の値が可能です。 • [Low]：イーサネットから供給されるアクセス ポイントの電力が低い。 • [Lower than 15.4 volts]：イーサネットから供給されるアクセス ポイントの電力が 15.4 V 未満。 • [Lower than 16.8 volts]：イーサネットから供給されるアクセス ポイントの電力が 16.8 V 未満。 • [Normal]：アクセス ポイントの操作に十分な電力が供給されている。 • [Not Applicable]：電源がイーサネットではない。

表 1-26　Lightweight アクセス ポイントの [General] タブのフィールド（続き）

フィールド	説明
Rogue Detection	不正検出が有効になっているかどうかを示します。 OfficeExtend アクセス ポイントについては、不正検出が自動的に無効になります。これらのアクセス ポイントは、住居環境で展開され、大量の不正デバイスを検出する可能性が高いためです。
OfficeExtend AP	アクセス ポイントが OfficeExtend アクセス ポイントとして有効になっているかどうかを示します。AP は、デフォルトで有効になっています。
Encryption	暗号化が有効になっているかどうかを示します。暗号化機能を有効または無効にするとアクセス ポイントが再起動し、それによってクライアントの接続が失われることになります。 DTLS データ暗号化は、セキュリティを維持するため、OfficeExtend アクセス ポイントで自動的に有効になります。暗号化は、Plus ライセンスが設定された 5500 シリーズ コントローラにアクセス ポイントが接続されている場合のみ使用できます。
Least Latency Join	アクセス ポイントは、プライオリティ順序検索（プライマリ、セカンダリ、ターシャリ コントローラ）から、遅延測定値が最善（最短遅延）のコントローラの検索に切り替えます。遅延が最短のコントローラが、最善のパフォーマンスを提供します。
Telnet Access	Telnet アクセスが有効になっているかどうかを示します。
SSH Access	SSH が有効になっているかどうかを示します。 OfficeExtend アクセス ポイントは、デフォルトのパスワードがアクセス ポイントで使用されている場合に外部アクセスを許可する可能性がある WAN に直接接続されていることがあります。そのため、OfficeExtend アクセス ポイントについては、Telnet および SSH のアクセスが自動的に無効になります。
Versions	
Software Version	コントローラで現在実行しているコードのオペレーティング システム リリースのバージョン番号。
Boot Version	オペレーティング システムのブートローダのバージョン番号。
Inventory Information	
AP Type	アクセス ポイントの種類
AP Model	アクセス ポイントのモデル番号。
Cisco IOS Version	Cisco IOS Release の詳細。
AP Certificate Type	自己署名または製造者がインストールした証明書。
FlexConnect Mode Supported	FlexConnect モードがサポートされているかどうかを示します。
wIPS Profile（該当する場合）	
Profile Name	wIPS プロファイルの詳細情報。
Profile Version	zIPS プロファイルのバージョン。
Unique Device Identifier (UDI)	
Name	アクセス ポイントの Cisco AP の名前。
Description	アクセス ポイントの説明。

表 1-26　Lightweight アクセス ポイントの [General] タブのフィールド（続き）

フィールド	説明
Product ID	注文可能な製品 ID
Version ID	製品 ID のバージョン
Serial Number	一意の製品シリアル番号
Run Ping Test Link	クリックするとアクセス ポイントに ping が実行されます。結果はポップアップ ダイアログボックスに表示されます。
Alarms Link	クリックすると、このアクセス ポイントに関連付けられたアラームが表示されます。
Events Link	クリックすると、このアクセス ポイントに関連付けられたイベントが表示されます。

表 1-27 で、[Monitor] > [Wireless Technologies] > [Access Point Radios] > [General] の Autonomous アクセス ポイントの各フィールドについて説明します。

表 1-27　Autonomous アクセス ポイントの [General] タブのフィールド

フィールド	説明
AP Name	オペレータが定義したアクセス ポイント名。
AP IP address and Ethernet MAC address	アクセス ポイントの IP アドレス、イーサネット MAC アドレス。
AP UpTime	アクセス ポイントが送受信できる状態になっている時間（日、時間、分、秒）を示します。
Map Location	アクセス ポイントのカスタマー定義の場所名。クリックするとマップ上で実際の場所が表示されます。
WGB Mode	アクセス ポイントがワーク グループ ブリッジ モードかどうかを示します。
SNMP Info	
SysObjectId	システム オブジェクト ID。
SysDescription	システム デバイスの種類とファームウェアの現在のバージョン。
SysLocation	デバイスが設置されている建物の名前や部屋など、デバイスの物理的な場所。
SysContact	デバイスを担当するシステム管理者の名前。
Versions	
Software Version	現在コントローラで実行されているコードのオペレーティング システムの release.version.dot.maintenance 番号。
CPU Utilization	指定した期間の最大、平均、および最小 CPU 使用率が表示されます。
Memory Utilization	指定した期間の最大、平均、および最小メモリ使用率が表示されます。
Inventory Information	
AP Type	AP タイプを表示します。
AP Model	AP モデル番号を表示します。
AP Serial Number	AP の一意のシリアル番号を表示します。
FlexConnect Mode Supported	選択した AP で FlexConnect モードがサポートされているかどうかを表示します。

表 1-27　Autonomous アクセス ポイントの [General] タブのフィールド（続き）

フィールド	説明
Unique Device Identifier (UDI)	
Name	アクセス ポイントの Cisco AP の名前。
Description	アクセス ポイントの説明。
Product ID	注文可能な製品 ID
Version ID	製品 ID のバージョン
Serial Number	一意の製品シリアル番号

[Monitor] > [Wireless Technologies] > [Access Point Radios] > [Interfaces]

表 1-28 で、[Monitor] > [Wireless Technologies] > [Access Point Radios] > [Interface] の各フィールドについて説明します。

表 1-28　[Interfaces] タブのフィールド

フィールド	説明
Interface	
Admin Status	イーサネット インターフェイスが有効になっているかどうかを示します。
Operational Status	イーサネット インターフェイスが動作可能かどうかを示します。
Rx Unicast Packets	受信したユニキャスト パケットの数を示します。
Tx Unicast Packets	送信したユニキャスト パケットの数を示します。
Rx Non-Unicast Packets	受信した非ユニキャスト パケットの数を示します。
Tx Non-Unicast Packets	送信した非ユニキャスト パケットの数を示します。
Radio Interface	
Protocol	802.11a/n または 802.11b/g/n。
Admin Status	アクセス ポイントが有効か無効かを示します。
CleanAir Capable	アクセス ポイントが CleanAir を使用できるかどうかを示します。
CleanAir Status	CleanAir のステータスを示します。
Channel Number	Cisco 無線がブロードキャストしているチャネルを示します。
Extension Channel	Cisco 無線がブロードキャストしているセカンダリ チャネルを示します。
Power Level	Access point transmit power level：1 = 国番号設定で許可される最大電力、2 = 50 % の電力、3 = 25 % の電力、4 = 6.25 ～ 12.5 % の電力、5 = 0.195 ～ 6.25 % の電力。
Channel Width	この無線インターフェイスのチャネル帯域幅を示します。デフォルトの設定は 20 MHz です。これはデフォルト値でもあります。最大設定値は、この無線がサポートする最大チャネル幅です。
Antenna Name	アンテナの種類を示します。

表 1-29 で、[Interface Properties] の各フィールドについて説明します。

表 1-29　[Interface Properties] フィールド

フィールド	説明
AP Name	アクセス ポイントの名前。
Link speed	インターフェイスの速度を Mbps 単位で示します。
RX Bytes	インターフェイス上で受信したエラーのないパケットの総バイト数を示します。
RX Unicast Packets	インターフェイス上で受信したユニキャスト パケットの総数を示します。
RX Non-Unicast Packets	インターフェイス上で受信した非ユニキャストまたはマルチキャスト パケットの総数を示します。
Input CRC	インターフェイス上で受信したパケット内の CRC エラーの総数を示します。
Input Errors	インターフェイスでの受信中に発生した、パケットのすべてのエラーの合計を示します。
Input Overrun	入力レートがレシーバのデータ処理能力を超えたために、レシーバ ハードウェアが受信データをハードウェア バッファに送信できなかった回数を示します。
Input Resource	インターフェイス上で受信したパケット内のリソース エラーの総数を示します。
Runts	メディアの最小パケット サイズよりも小さいために廃棄されたパケット数を示します。
Throttle	インターフェイスが、送信中のパケットが多すぎるため、配信速度を落とすように、送信 NIC にアドバイスを送信した合計回数を示します。
Output Collision	イーサネット コリジョンにより再送信したパケットの総数を示します。
Output Resource	インターフェイス上で送信したパケットのリソース エラーの総数を示します。
Output Errors	最終的にインターフェイスからのパケットの送信ができなかった原因となるエラーの合計数を示します。
Operational Status	AP 上の物理イーサネット インターフェイスの動作状態を示します。
Duplex	インターフェイスのデュプレックス モードを示します。
TX Bytes	インターフェイス上で送信したエラーのないパケットの総バイト数を示します。
TX Unicast Packets	インターフェイス上で送信したユニキャスト パケットの総数を示します。
TX Non-Unicast Packets	インターフェイス上で送信した非ユニキャストまたはマルチキャスト パケットの総数を示します。
Input Aborts	インターフェイス上で受信中に中断されたパケットの総数を示します。
Input Frames	インターフェイス上で受信した、CRC エラーがあり、オクテット数が整数でないパケットの総数を示します。
Input Drops	インターフェイス上での受信中に、キューが一杯だったためにドロップされたパケットの総数を示します。
Unknown Protocol	不明なプロトコルが原因でインターフェイス上で廃棄されたパケットの総数を示します。
Giants	メディアの最大パケット サイズを超過したために廃棄されたパケット数を示します。
Interface Resets	インターフェイスが完全にリセットされた回数を示します。
Output No Buffer	バッファ領域がなかったために廃棄されたパケットの総数を示します。

表 1-29　[Interface Properties] フィールド（続き）

フィールド	説明
Output Underrun	ルータの処理能力を超えた速度でトランスミッタが動作した回数を示します。
Output Total Drops	インターフェイスからの送信中に、キューが一杯だったためにドロップされたパケットの総数を示します。

[Monitor] > [Wireless Technologies] > [Access Point Radios] > [CDP Neighbors]

表 1-30 で、[Monitor] > [Wireless Technologies] > [Access Point Radios] > [CDP Neighbors] の各フィールドについて説明します。

表 1-30　[CDP Neighbors] タブのフィールド

フィールド	説明
AP Name	アクセス ポイントに割り当てられた名前。
AP IP Address	アクセス ポイントの IP アドレス。
Port No	アクセス ポイントに接続されているか割り当てられているポート番号。
Local Interface	ローカル インターフェイスを示します。
Neighbor Name	隣接するシスコ デバイスの名前。
Neighbor Address	隣接するシスコ デバイスのネットワーク アドレス。
Neighbor Port	隣接するシスコ デバイスのポート。
Duplex	全二重なのか半二重なのかを示します。
Interface Speed	インターフェイスが動作している速度。

[Monitor] > [Wireless Technologies] > [Access Point Radios] > [Current Associated Client]

表 1-31 で、[Monitor] > [Wireless Technologies] > [Access Point Radios] > [Current Associated Clients] の各フィールドについて説明します。

注　現在関連付けられているクライアントの IP アドレスは、(現在関連付けられているクライアントが起動された)現在のスイッチがそのクライアントの IP アドレスを取得している場合にのみ表示されます。

表 1-31　[Current Associated Clients] タブのフィールド

フィールド	説明
Username	関連付けられているクライアントのユーザ名。
IP Address	関連付けられているクライアントの IP アドレス。
Client MAC Address	関連付けられているクライアントの MAC アドレス
Association Time	アソシエーションの日時。

表 1-31　[Current Associated Clients] タブのフィールド（続き）

フィールド	説明
UpTime	アソシエーションの継続時間。
SSID	ユーザ定義の SSID 名。
SNR (dB)	関連付けられているクライアントの、信号対雑音比（dB 単位）。
RSSI	受信信号強度インジケータ（dBm）。
Bytes Tx	イーサネット インターフェイスをいずれかの方法で経由して渡されたデータの総量。
Bytes Rx	イーサネット インターフェイスをいずれかの方法で経由して受信したデータの総量。
アクセス ポイントがコントローラに関連付けられていない場合、コントローラ自身ではなく、データベースを使用してデータが取得されます。アクセス ポイントが関連付けられていない場合、次のフィールドが表示されます。	
User Name	クライアントのユーザ名。
IP Address	ローカル IP アドレス。
Client MAC Address	Client MAC Address
Association Time	クライアント関連付けのタイムスタンプ。
Session Length	セッションの時間の長さ。
SSID	ユーザ定義の SSID 名。
Protocol	関連付けられているクライアントのプロトコル。

[Monitor] > [Wireless Technologies] > [Access Point Radios] > [SSID]

表 1-32 で、[Monitor] > [Wireless Technologies] > [Access Point Radios] > [SSID] の各フィールドについて説明します。

表 1-32　[SSID] タブのフィールド

フィールド	説明
SSID	アクセス ポイントの無線によってブロードキャストされているサービス セット ID。
SSID Vlan	アクセス ポイント上の SSID は、特定の VLAN ID または名前を認識するために設定されます。
SSID Vlan Name	アクセス ポイント上の SSID は、特定の VLAN ID または名前を認識するために設定されます。
MB SSID Broadcast	DDIS ブロードキャストが無効になっていると、ワイヤレス クライアントが SSID を取得済みであるか、AP に関連付けられているクライアントからのトラフィックをモニタするツールを使用していない限り、AP は基本的に表示されません。
MB SSID Time Period	SSID 内の内部通信が動作を継続する時間。

[Rogue AP Alarms] ページ

次の表で、[Rogue AP Alarms] ページにあるフィールドについて説明します。

表 1-33　[Rogue AP Alarms] ページのフィールド

フィールド	説明
Severity	アラームの重大度をアイコンで表示します。Severity Configuration 機能を使用して、次の不正アクセス ポイント アラーム タイプの重大度を決定できます。 • Rogue detected • Rogue detected contained • Rogue detected on network
Rogue MAC Address	不正アクセス ポイントの MAC アドレスを示します。
Vendor	不正アクセス ポイントのベンダー名または [Unknown]
Classification Type	[Pending]、[Malicious]、[Friendly]、または [Unclassified]。
Radio Type	この不正アクセス ポイントに該当するすべての無線タイプをリストします。
Strongest AP RSSI	その不正の存続期間にわたってこの不正アクセス ポイントに最も強力な AP RSSI を表示します。不正アクセス ポイントと、建物または場所の間に存在する最短距離を示すために、不正の存続期間を超えて最も強い AP RSSI が表示されます。RSSI が大きいほど、場所は近くなります。
No. of Rogue Clients	この不正アクセス ポイントに関連付けられた不正クライアントの数を示します。この数は、Prime Infrastructure データベースから取得します。2 時間ごとに更新されます。この数はリアルタイムの数であり、この不正アクセス ポイントの [Alarm Details] ページを開くたびに更新されます。
Owner	このアラームを割り当てる個人の名前、または(空白)。
Last Seen Time	不正アクセス ポイントが最後に確認された日時を表示します。
State	アラームの状態を示します。可能な状態は、不正アクセス ポイントの分類タイプによって異なります。 • 悪意のある不正アクセス ポイントの状態には、Alert、Contained、Threat、Contained Pending、および Removed があります。 • 危険性のない不正アクセス ポイントの状態には、Internal、External、および Alert があります。 • 未分類の不正アクセス ポイントの状態には、Pending、Alert、Contained、および Contained Pending があります。
SSID	不正アクセス ポイントの無線によってブロードキャストされるサービス セット識別子を示します。SSID がブロードキャストされていない場合は空欄になります。
Map Location	この不正アクセス ポイントのマップ場所を表示します。
Acknowledged	対象ユーザがこのアラームを確認済みであるかどうかが表示されます。 [Alarm Summary] ページに表示されないように、アラームを承認できます。アラームは Prime Infrastructure 内に残るため、アラーム検索機能を使用すると、確認応答したすべてのアラームを検索できます。

アラーム重大度インジケータ アイコン

表 1-34　アラーム重大度インジケータ アイコン

アイコン	意味
	Critical
	Major
	Minor
	警告
	情報
	不明（Unknown） **注**　コントローラがダウンした場合、コントローラ インベントリ ダッシュレットでコントローラのステータスが重大として表示されます。しかし、無線インベントリ ダッシュレットでは、最後の既知のステータスのままになります。[Monitor] > [AP] ページには、AP アラーム ステータスが「Unknown」と表示されます。
	クリア：不正がどのアクセス ポイントでも検出されなくなった場合に表示されます。 **注**　不正は、複数のアクセス ポイントによって検出されることがあります。1 つのアクセス ポイントが不正を検出しなくなっても、他のアクセス ポイントが検出する場合は、クリアは送信されません。 **注**　不正の重大度がクリアされると、アラームは 30 日後に Prime Infrastructure から削除されます。

不正 AP アラームのコマンドの選択

1 つ以上のアラームをそれぞれ対応するチェックボックスをオンにして選択し、次のドリップダウン リストからいずれかのコマンドを選択します。

表 1-35　不正 AP アラームのコマンド ドロップダウン メニュー

フィールド	説明
Change Status	• [Acknowledge]：アラームに確認応答し、[Alarm Summary] ページに表示されないようにします。アラームは Prime Infrastructure 内に残るため、アラーム検索機能を使用すると、確認応答したすべてのアラームを検索できます。 • [Unacknowledge]：すでに認知しているアラームを未認知にします。 • [Clear]：選択したアラームをクリアします。アラームがどのアクセス ポイントでも検出されなくなったことを示します。重大度が [Clear] になると、アラームは 30 日経過後に Prime Infrastructure から削除されます。
Change State	• [Unclassified - Alert]：不正アクセス ポイントに最低の脅威とするタグを設定し、その不正アクセス ポイントの監視を継続して、封じ込めをオフにするには、このコマンドを選択します。不正アクセス ポイントのMAC アドレスを表示します。 • [Malicious - Alert]：不正アクセス ポイントに「悪意がある」とするタグを設定するには、このコマンドを選択します。 • [Friendly - Internal]：不正アクセス ポイントに内部とするタグを設定し、[Known Rogue AP] リストに追加して封じ込めをオフにするには、このコマンドを選択します。 • [Friendly - External]：不正アクセス ポイントに外部とするタグを設定し、[Known Rogue AP] リストに追加して封じ込めをオフにするには、このコマンドを選択します。 • [Refresh from Network]：ネットワークを更新します。
Assign	• [Assign to me]：選択したアラームを現在のユーザに割り当てます。 • [Unassign]：選択したアラームの割り当てを解除します。 • [Select Owner]：選択したアラームを特定のユーザに割り当てます。
Annotation	メモを入力し、そのメモを保存して表示するには [Post] をクリックします。メモを保存せずにページを閉じるには [Close] をクリックします。
Email Notification	[Monitor] > [Monitoring Tools] > [Alarms and Events] > [Email Notification] ページに移動し、電子メールでの通知を設定します。

[Rogue AP Alarm Details] ページのドロップダウン メニュー

表 1-36　[Rogue AP Alarm Details] ページのメニュー

フィールド	説明
Change Status	• [Acknowledge]:アラームに確認応答し、[Alarm Summary] ページに表示されないようにします。アラームは Prime Infrastructure 内に残るため、アラーム検索機能を使用すると、確認応答したすべてのアラームを検索できます。 • [Unacknowledge]:すでに認知しているアラームを未認知にします。 • [Clear]:選択したアラームをクリアします。アラームがどのアクセス ポイントでも検出されなくなったことを示します。重大度が [Clear] になると、アラームは 30 日経過後に Prime Infrastructure から削除されます。 • [Set State to 'Unclassified - Alert']:不正アクセス ポイントに最低の脅威とするタグを設定し、その不正アクセス ポイントの監視を継続して、封じ込めをオフにするには、このコマンドを選択します。 • [Set State to 'Malicious - Alert']:不正アクセス ポイントに「悪意がある」とするタグを設定するには、このコマンドを選択します。 • [Set State to 'Friendly - Internal']:不正アクセス ポイントに内部とするタグを設定し、[Known Rogue AP] リストに追加して封じ込めをオフにするには、このコマンドを選択します。 • [Set State to 'Friendly - External']:不正アクセス ポイントに外部とするタグを設定し、[Known Rogue AP] リストに追加して封じ込めをオフにするには、このコマンドを選択します。 • [Refresh from Network]:アラームの詳細情報を更新します。
Assign	• [Assign to me]:選択したアラームを現在のユーザに割り当てます。 • [Unassign]:選択したアラームの割り当てを解除します。 • [Select Owner]:所有者を割り当てます。
View	• [View Detecting AP on Network]: • [View Details by Controller]:
AP Containment	• [1 AP Containment]:不正アクセス ポイントを 1 つのアクセス ポイントで封じ込めます。(最小封じ込めレベル)。 • [2 AP Containment]:不正アクセス ポイントを 2 つの Cisco 1000 シリーズ Lightweight アクセス ポイントで封じ込めます。 • [3 AP Containment]:不正アクセス ポイントを 3 つの Cisco 1000 シリーズ Lightweight アクセス ポイントで封じ込めます。 • [4 AP Containment]:不正アクセス ポイントを 4 つの Cisco 1000 シリーズ Lightweight アクセス ポイントで封じ込めます。(最大封じ込めレベル)。 不正アクセス ポイントの脅威が高いほど、高い封じ込め処理が必要です。 不正アクセス ポイントの封じ込めは法的責任を伴う場合があります。AP 封じ込めコマンドのいずれかを選択すると、メッセージ「Containing a Rogue AP may have legal consequences. Do you want to continue?」が表示されます。処理を続行する場合は [OK] をクリックします。アクセス ポイントを封じ込めない場合は [Cancel] をクリックします。

[Ad hoc Rogue Alarm Details]

次の表で、[Ad hoc Rogue Alarm Details] ページにあるフィールドについて説明します。

表 1-37　[Ad hoc Rogue Alarm] のフィールド

フィールド	説明
General	
Rogue MAC Address	不正アクセス ポイントの MAC アドレスを表示します。
Vendor	不正アクセス ポイントのベンダー名または [Unknown] を表示します。 Airlink の不正アクセス ポイントのアラームは Airlink ではなく、Alpha と表示されます。
Rogue Type	AP など、不正のタイプを表示します。
On Network	不正検出がどのように発生したかを表示します。
Controller	不正を検出したコントローラの名前を表示します([Yes] または [No])。
Switch Port Trace	不正を検出したスイッチ ポート トレースを表示します。スイッチ ポート トレースのタイプは次のいずれかです。 – Traced but not found – Traced and found – Not traced
Owner	所有者の名前を表示します。空欄のままの場合もあります。
Acknowledged	対象ユーザがこのアラームを確認済みであるかどうかが表示されます。[Alarm Summary] ページに表示されないように、アラームを承認できます。アラームは Prime Infrastructure 内に残るため、アラーム検索機能を使用すると、確認応答したすべてのアラームを検索できます。
Classification Type	不正アクセス ポイントの分類タイプを表示します。次の分類があります。 – Malicious – Friendly – Unclassified
State	アラームの状態を表示します。不正アクセス ポイントの分類タイプによって、表示される状態が異なります。
SSID	不正アクセス ポイントの無線によってブロードキャストされるサービス セット識別子を表示します。このフィールドは、SSID ブロードキャストでない場合は空欄のままになります。
Channel Number	不正アクセス ポイントのチャネルを表示します。
Containment Level	不正アクセス ポイントの封じ込めレベルを表示します。
Radio Type	この不正アクセス ポイントに該当するすべての無線タイプをリストします。
Strongest AP RSSI	この不正アクセス ポイントの不正の存続期間にわたって最も強力な AP RSSI を表示します。 不正の存続期間で最も強い AP RSSI は、不正アクセス ポイントとユーザのビルディングまたは場所間に存在した最も近い距離を示します。RSSI が大きいほど、場所は近くなります。

表 1-37　[Ad hoc Rogue Alarm] のフィールド（続き）

フィールド	説明
No. of Rogue Clients	この不正アクセス ポイントに関連付けられた不正クライアントの数を表示します。 これは、唯一のリアルタイム フィールドです。これは、この不正アクセス ポイントの [Alarm Details] ページを開くたびに更新されます。[Alarm Details] ページのその他すべてのフィールドは、ポーリングによってデータが設定され、2 時間ごとに更新されます。
First Seen Time	不正アクセス ポイントが最初に検出された日時を表示します。この情報は、コントローラから入力されます。
Last Seen Time	不正アクセス ポイントが最後に検出された日時を表示します。この情報は、コントローラから入力されます。
Modified	アラーム イベントがいつ変更されたかを表示します。
Generated By	アラーム イベントがどのように生成されたか（NMS かトラップからか）を表示します。 – NMS（ネットワーク管理システム - Prime Infrastructure）：ポーリングにより生成。Prime Infrastructure は、コントローラを定期的にポーリングして、イベントを生成します。Prime Infrastructure は、トラップを無効にするか、これらのイベントのトラップが失われるとイベントを生成します。この場合、[Benerated By] には NMS と表示されます。 – [Trap]：コントローラによって生成されます。Prime Infrastructure は、これらのトラップを処理して、対応するイベントを発生させます。この場合、「Generated by」は Controller です。
Severity	アラームの重大度を表示します。
Previous Severity	アラームの以前の重大度を表示します。 – Critical – Major – Minor – Clear
Event Details	イベントの詳細情報を表示します。
Rogue AP History	不正 AP アラーム履歴の詳細情報を表示します。
Switch Port Trace Status	スイッチ ポート トレースのステータスを表示します。スイッチ ポート トレースのステータスに含まれる可能性がある項目は次のとおりです。 – Traced, but not found – Traced and found, Not traced – Failed
Rogue Clients	このアクセス ポイントの不正クライアントを表示します。クライアント MAC アドレス、クライアントが最後に確認された日時、クライアントの現在のステータスなどが含まれます。
Message	この不正アクセス ポイントに関する最新のメッセージを表示します。次についてのメッセージが送信されます。 – 最初に検出された不正アクセス ポイント – 送信されたトラップ – 変更された状態

表 1-37　[Ad hoc Rogue Alarm] のフィールド（続き）

フィールド	説明
Annotations	この不正アクセス ポイントに関する現在のメモを表示します。 新しい注釈を追加するには、[New Annotation] をクリックします。メモを入力し、そのメモを保存して表示するには [Post] をクリックします。メモを保存せずにページを閉じるには [Cancel] をクリックします。
Location Notifications	クライアントに対して記録されている位置の通知の数が表示されます。
Location	可能な場合は、場所情報を表示します。

[Rogue AP History Details] ページ

次の表で、[Rouge AP History Details] ページにあるフィールドについて説明します。

表 1-38　Rogue AP History Details

フィールド	説明
Severity	アラームの重大度。
Rogue MAC Address	不正アクセス ポイントの MAC アドレス。
Classification Type	Malicious（危険性あり）、Friendly（危険性なし）、Unclassified（未分類）。
Radio Type	この不正アクセス ポイントに該当するすべての無線タイプをリストします。
Strongest AP RSSI	この不正アクセス ポイントの不正の存続期間にわたって最も強力な AP RSSI を表示します。不正の存続期間で最も強い AP RSSI は、不正アクセス ポイントとユーザのビルディングまたは場所間に存在した最も近い距離を示します。RSSI が大きいほど、場所は近くなります。
No. of Rogue Clients	この不正アクセス ポイントに関連付けられた不正クライアントの数を示します。
First Seen Time	不正アクセス ポイントが最初に検出された日時を示します。この情報は、コントローラから入力されます。
Last Seen Time	不正アクセス ポイントが最後に検出された日時を示します。この情報は、コントローラから入力されます。
State	アラームの状態を示します。可能な状態は、不正アクセス ポイントの分類タイプによって異なります。
SSID	不正アクセス ポイント無線によってブロードキャストされているサービス セット ID（SSID）。SSID がブロードキャストされない場合は空欄になります。
Category	このアラームのカテゴリ（Security や Prime Infrastructure など）を示します。
On Network	不正検出がどのように発生したかを示します。 • [Controller]：コントローラが不正を検出しました（[Yes] または [No]）。 • [Switch Port Trace]：不正がスイッチ ポート トレースによって検出されました。[Traced but not found]、[Traced and found]、[Not traced] のいずれかで示されます。
Channel Number	アドホック不正のチャネルを示します。
Containment Level	アドホック不正の封じ込めレベル、または [Unassigned] を示します。
Switch Port Trace Status	スイッチ ポート トレースのステータスを示します。スイッチ ポート トレース ステータスには、[Traced, but not found]、[Traced and found]、[Not traced]、[Failed] があります。

[Rogue AP Event History Details] ページ

次の表で、[Rouge AP Event History Details] ページにあるフィールドについて説明します。

表 1-39　Rogue AP Event History Details

フィールド	説明
Severity	アラームの重大度。
Rogue MAC Address	不正アクセス ポイントの MAC アドレス。
Vendor	不正アクセス ポイントのベンダー名または [Unknown]。
Classification Type	Malicious（危険性あり）、Friendly（危険性なし）、Unclassified（未分類）。
On Network	不正検出が発生したかどうかを示します。コントローラが不正を検出しました（[Yes] または [No]）。
Radio Type	この不正アクセス ポイントに該当するすべての無線タイプをリストします。
Date/Time	イベントが生成された日時。
State	アラームの状態を示します。可能な状態は、不正アクセス ポイントの分類タイプによって異なります。
SSID	不正アクセス ポイント無線によってブロードキャストされているサービス セット ID（SSID）。SSID がブロードキャストされない場合は空欄になります。

[Ad hoc Rogue Alarms] ページ

次の表で、[Ad hoc Rogue Alarms] ページにあるフィールドについて説明します。

表 1-40　Ad hoc Rogue Alarms Details

フィールド	説明
Severity	アラームの重大度をアイコンで表示します。Severity Configuration 機能を使用して、次の不正アクセス ポイント アラーム タイプの重大度を決定できます。 • Rogue detected • Rogue detected contained • Rogue detected on network
Rogue MAC Address	不正の MAC アドレスを示します。
Vendor	アドホック不正ベンダー名または [Unknown] を示します。
Radio Type	この不正アクセス ポイントに該当するすべての無線タイプをリストします。
Strongest AP RSSI	この不正の存続期間にわたって、この不正の最も強力な AP RSSI を表示します。不正の存続期間で最も強い AP RSSI は、不正とユーザのビルディングまたは場所間に存在した最も近い距離を示します。RSSI が大きいほど、場所は近くなります。
No. of Rogue Clients	この不正アクセス ポイントに関連付けられた不正クライアントの数を示します。不正クライアントの数は、[Alarm Details] ページの唯一のリアルタイム フィールドです。これは、この不正アクセス ポイントの [Alarm Details] ページを開くたびに更新されます。 [Alarm Details] ページのその他すべてのフィールドは、ポーリングによってデータが設定され、2 時間ごとに更新されます。

表 1-40　Ad hoc Rogue Alarms Details（続き）

フィールド	説明
Owner	所有者を示すか、空欄です。
Last Seen Time	不正アクセス ポイントが最後に確認された日時を表示します。
State	アラームの状態を示します。アドホック不正の可能な状態には、[Threat]、[Alert]、[Internal]、[External]、[Contained]、[Contained Pending]、および [Removed] があります。
SSID	不正アドホック無線によってブロードキャストされるサービス セット識別子。ブロードキャストがない場合は空白になります。
Map Location	このアドホック不正のマップ場所を示します。
Acknowledged	対象ユーザがこのアラームを確認済みであるかどうかが表示されます。 [Alarm Summary] ページに表示されないように、アラームを承認できます。アラームは Prime Infrastructure 内に残るため、アラーム検索機能を使用すると、確認応答したすべてのアラームを検索できます。

アドホック不正 AP アラームのコマンドの選択

1 つ以上のアラームをそれぞれ対応するチェックボックスをオンにして選択し、次のドリップダウン リストからいずれかのコマンドを選択します。

表 1-41　アドホック不正 AP アラームのコマンド

フィールド	説明
Change Status	• [Acknowledge]：アラームに確認応答し、[Alarm Summary] ページに表示されないようにします。アラームは Prime Infrastructure 内に残るため、アラーム検索機能を使用すると、確認応答したすべてのアラームを検索できます。 • [Unacknowledge]：すでに認知しているアラームを未認知にします。 • [Clear]：選択したアラームをクリアします。アラームがどのアクセス ポイントでも検出されなくなったことを示します。重大度が [Clear] になると、アラームは 30 日経過後に Prime Infrastructure から削除されます。
Change State	• [Unclassified - Alert]：不正アクセス ポイントに最低の脅威とするタグを設定し、その不正アクセス ポイントの監視を継続して、封じ込めをオフにするには、このコマンドを選択します。不正アクセス ポイントのMAC アドレスを表示します。 • [Malicious - Alert]：不正アクセス ポイントに「悪意がある」とするタグを設定するには、このコマンドを選択します。 • [Friendly - Internal]：不正アクセス ポイントに内部とするタグを設定し、[Known Rogue AP] リストに追加して封じ込めをオフにするには、このコマンドを選択します。 • [Friendly - External]：不正アクセス ポイントに外部とするタグを設定し、[Known Rogue AP] リストに追加して封じ込めをオフにするには、このコマンドを選択します。 • [Refresh from Network]：
Assign	• [Assign to me]：選択したアラームを現在のユーザに割り当てます。 • [Unassign]：選択したアラームの割り当てを解除します。

表 1-41　アドホック不正 AP アラームのコマンド（続き）

フィールド	説明
Annotation	メモを入力し、そのメモを保存して表示するには [Post] をクリックします。メモを保存せずにページを閉じるには [Close] をクリックします。
Delete	選択したアラームを削除します。
Email Notification	[Monitor] > [Alarms and Events] > [Email Notification] ページに移動し、電子メールでの通知を設定します。

アドホック不正アラームの詳細情報の表示

表 1-42　[Ad hoc Rogue Alarm Details] ページの説明

フィールド	説明
Rogue MAC Address	不正の MAC アドレスを示します。
Vendor	アドホック不正ベンダー名または [Unknown] を示します。
On Network	不正検出がどのように発生したか(コントローラかスイッチ ポート トレースか)を示します。 スイッチ ポート トレースは、重大度、状態などの不正の属性を更新しません。不正の属性はスイッチ ポート トレースで更新されないため、スイッチ ポート トレースを使用して、不正が「ネットワーク上にある」と検出された場合、アラームは生成されません。
Owner	所有者を示すか、空欄です。
Acknowledged	ユーザがアラームに確認応答したかどうかを示します。 アラームに確認応答すると、[Alarm Summary] ページに表示されません。アラームは Prime Infrastructure 内に残るため、アラーム検索機能を使用すると、確認応答したすべてのアラームを検索できます。
State	アラームの状態を示します。アドホック不正の可能な状態には、[Threat]、[Alert]、[Internal]、[External]、[Contained]、[Contained Pending]、および [Removed] があります。
SSID	不正アドホック無線によってブロードキャストされるサービス セット識別子。ブロードキャストがない場合は空白になります。
Channel Number	アドホック不正のチャネルを示します。
Containment Level	アドホック不正の封じ込めレベル、または [Unassigned] を示します。
Radio Type	この不正アクセス ポイントに該当するすべての無線タイプをリストします。
Strongest AP RSSI	この不正の存続期間にわたって、この不正の最も強力な AP RSSI を表示します。不正の存続期間で最も強い AP RSSI は、不正とユーザのビルディングまたは場所間に存在した最も近い距離を示します。RSSI が大きいほど、場所は近くなります。
No. of Rogue Clients	この不正アクセス ポイントに関連付けられた不正クライアントの数を示します。不正クライアントの数は、[Alarm Details] ページの唯一のリアルタイム フィールドです。これは、この不正アクセス ポイントの [Alarm Details] ページを開くたびに更新されます。 [Alarm Details] ページのその他すべてのフィールドは、ポーリングによってデータが設定され、2 時間ごとに更新されます。
Created	アラーム イベントがいつ作成されたかを示します。

表 1-42　[Ad hoc Rogue Alarm Details] ページの説明（続き）

フィールド	説明
Modified	アラーム イベントがいつ変更されたかを示します。
Generated By	アラーム イベントがどのように生成されたか(NMS かトラップからか)を示します。
Severity	アラームの重大度を示します。
Previous Severity	アラームの以前の重大度:[Critical]、[Major]、[Minor]、[Clear] 色分けして表示されます。
Last Seen Time	不正アクセス ポイントが最後に確認された日時を表示します。
Location Notification	クライアントに対して記録されている位置の通知の数が表示されます。リンクをクリックすると、通知が表示されます。
Map Location	このアドホック不正のマップ場所を示します。
Rogue Clients Details	このアクセス ポイントの不正クライアントをリストします。クライアント MAC アドレス、クライアントが最後に確認された日時、クライアントの現在のステータスなどが含まれます。
Message	アラームについての説明情報を示します。
Help	アラームについての最新情報を示します。
Event History	イベント履歴を表示します。
Annotations	選択したアラームの既存のメモをリストします。

[Chokepoints] ページ

次の表に、チョークポイントが表示されるページのフィールドを示します。

表 1-43　[Chokepoints] フィールドの説明

フィールド	説明
MAC Address	チョークポイントの MAC アドレス。
Chokepoint Name	チョークポイントのユーザ定義の名前。
Entry/Exit Chokepoint	チョークポイントが Entry/Exit チョークポイントかどうかを示します。
Static IP	チョークポイントのスタティック IP アドレス。
Map Location	チョークポイントの場所を示すマップへのリンク。

[AP Detected Interferers] ページ

表 1-44　[AP Detected Interferers] ページのフィールド

フィールド	説明
Interferer ID	干渉の一意の識別子。これは、疑似乱数によって生成される ID です。MAC アドレスに似ていますが、例えば Bluetooth ヘッドセットで使用されるものなど、実際のアドレスではありません。
Type	干渉のカテゴリを示します。デバイスのタイプの詳細を参照するには、ここをクリックします。ポップアップ ウィンドウに詳細が表示されます。次のカテゴリがあります。 • [Bluetooth link]：Bluetooth リンク（802.11b/g/n のみ） • [Microwave Oven]：電子レンジ（802.11b/g/n のみ） • [802.11 FH]：802.11 周波数ホッピング デバイス（802.11b/g/n のみ） • [Bluetooth Discovery]：Bluetooth 検出（802.11b/g/n のみ） • [TDD Transmitter]：時分割複信（TDD）トランスミッタ • [Jammer]：電波妨害デバイス • [Continuous Transmitter]：連続トランスミッタ • [DECT-like Phone]：Digital Enhanced Cordless Communication（DECT）対応電話 • [Video Camera]：ビデオ カメラ • [802.15.4]：802.15.4 デバイス（802.11b/g/n のみ） • [WiFi Inverted]：スペクトル反転 Wi-Fi 信号を使用するデバイス • [WiFi Invalid Channel]：非標準の Wi-Fi チャネルを使用するデバイス • [SuperAG]：802.11 SuperAG デバイス • [Canopy]：Motorola Canopy デバイス • [Radar]：レーダー デバイス（802.11a/n のみ） • [XBox]：Microsoft Xbox（802.11b/g/n のみ） • [WiMAX Mobile]：WiMAX モバイル デバイス（802.11a/n のみ） • [WiMAX Fixed]：WiMAX 固定デバイス（802.11a/n のみ） • [WiFi AOCI]：AOCI を使用する WiFi デバイス • 未分類
Status	干渉デバイスのステータスを示します。 • [Active]：CleanAir 対応アクセス ポイントにより現在干渉源が検出されていることを示します。 • [Inactive]：CleanAir 対応のアクセス ポイントでは干渉が検出されなくなった、または、Prime Infrastructure では到達できなくなったことを示します。
Severity	干渉デバイスの重大度ランキングを表示します。
Affected Band	このデバイスが干渉している帯域を表示します。
Affected Channels	影響を受けるチャネルを表示します。
Duty Cycle（%）	干渉デバイスのデューティ サイクル（% 単位）
Discovered	検出された時刻を表示します。

表 1-44　[AP Detected Interferers] ページのフィールド（続き）

フィールド	説明
Last Updated	干渉が最後に検出された時刻。
Floor	干渉デバイスが存在する場所。

[AP Detected Interferers Details] ページ

表 1-45　[AP Detected Interferers Details] ページのフィールド

フィールド	説明
Interferer Properties	[Type]：AP により検出された干渉デバイスのタイプが表示されます。
Status	干渉デバイスのステータス。干渉デバイスのステータスを示します。 • [Active]：CleanAir 対応アクセス ポイントにより現在干渉源が検出されていることを示します。 • [Inactive]：CleanAir 対応のアクセス ポイントでは干渉が検出されなくなった、または、Prime Infrastructure では到達できなくなったことを示します。 • [Severity]：干渉デバイスの重大度ランクを示します。 • [Duty Cycle (%)]：干渉デバイスのデューティ サイクル（パーセンテージ）。 • [Affected Band]：このデバイスが干渉している帯域を表示します。 • [Affected Channels]：影響を受けるチャネルを表示します。 • [Discovered]：検出された時刻を表示します。 • [Last Updated]：干渉源が最後に検出された時刻。
Status	干渉デバイスのステータスを示します。 • [Active]：CleanAir 対応アクセス ポイントにより現在干渉源が検出されていることを示します。 • [Inactive]：CleanAir 対応のアクセス ポイントでは干渉が検出されなくなった、または、Prime Infrastructure では到達できなくなったことを示します。
Location	• [Floor]：この干渉デバイスが検出されたロケーション。 • [Last Located At]：干渉デバイスが最後に検出された時刻。 • [On MSE]：この干渉デバイスが検出されたモビリティ サーバ エンジン。
Clustering Information	• [Clustered By]：アクセス ポイントからの干渉情報を収集したコントローラまたは MSE の IP アドレスが表示されます。 • [Detecting APs]：干渉デバイスを検出したアクセス ポイントの詳細情報を表示します。詳細情報には、[Access Point Name (Mac)]、[Severity]、および [Duty Cycle(%)] などが含まれます。
Details	干渉タイプについての簡単な説明を表示します。

[Monitor] > [Interferers] > [Interference Device ID] > [Location History]

このページを表示するには、[Monitor] > [Interferers] > [Interference Device ID] の順に選択し、[Select a command] ドロップダウン リストから [Location History] を選択し、[Go] をクリックします。

表 1-46　[AP Detected Interferers Details Location History] ページのフィールド

フィールド	説明
Interferer Information	干渉デバイスについての基本情報を表示します。 • [Data Collected At]:データが収集された時点のタイムスタンプ。 • [Type]:干渉デバイスのタイプ。 • [Severity]:干渉デバイスの重大度インデックス。 • [Duty Cycle]:干渉デバイスのデューティ サイクル(パーセンテージ)。 • [Affected Channels]:影響を受けるチャネルのカンマ区切りリスト。
Interferer Location History	干渉デバイスの場所の履歴を表示します。 • Time Stamp • Floor
Clustering Information	[Clustered By]:アクセス ポイントからの干渉情報を収集したコントローラまたは MSE の IP アドレスが表示されます。
Detecting APs	• [AP Name]:干渉デバイスを検出したアクセス ポイント。 • [Severity]:干渉デバイスの重大度インデックス。 • [Duty Cycle(%)]:干渉デバイスのデューティ サイクル(パーセンテージ)。
Location	• [Location Calculated At]:この情報が生成された時点のタイムスタンプを表示します。 • [Floor]:干渉デバイスのロケーション情報を表示します。 • 干渉デバイスのロケーションがマップにグラフィカルに表示されます。イメージを拡大表示するには [Enlarge] リンクをクリックします。

[Spectrum Experts] > [Summary]

[Spectrum Experts] > [Summary] ページはデフォルトのページで、システムに追加された Spectrum Experts のテーブルを表示します。この表には、次の Spectrum Expert の情報が記載されています。

表 1-47　[Spectrum Experts Summary] ページのフィールド

フィールド	説明
Host Name	追加された方法に応じて、ホスト名または IP アドレスを表示します。「[Spectrum Experts Details] ページ」ページにアクセスするには、ホスト名をクリックします。
Active Interferers	Spectrum Experts が検出している干渉の現在の数を示します。
Affected APs	検出された干渉によって影響を受けた可能性があり、Spectrum Expert で確認したアクセス ポイントの数。

表 1-47　[Spectrum Experts Summary] ページのフィールド（続き）

フィールド	説明
Alarms	Spectrum Expert が確認したアクティブな干渉トラップの数。クリックすると、この Spectrum Expert のアクティブ アラームに対してフィルタリングされている [Alarm] ページへアクセスします。
Reachability Status	Spectrum Expert が実行しており、Prime Infrastructure へデータを送信している場合は、緑色で [Reachable] と表示されます。それ以外の場合は、赤で [Unreachable] と表示されます。
Location	Spectrum がワイヤレス クライアントの場合は、Spectrum Expert の場所を表示するリンクが使用できます。Spectrum Expert の周囲の赤いボックスは、有効な範囲を示します。クリックすると、マップに配置された最も近いアクセス ポイントにアクセスできます。

[Interferers] > [Summary]

[Interferers] > [Summary] ページに、30 日間にわたって検出されたすべての干渉のリストを表示します。この表には、次のような干渉源の情報が記載されています。

表 1-48　[Interferes Summary] ページのフィールド

フィールド	説明
Interferer ID	異なる Spectrum Expert 間で一意の識別子。これは、疑似乱数によって生成される ID です。MAC アドレスに似ていますが、実際のアドレスではなく、干渉デバイスの検出に使用できます。
Category	干渉のカテゴリを示します。カテゴリには、[Bluetooth]、[Cordless Phones]、[Microwave Ovens]、[802.11 FH]、[Generic - Fixed-Frequency]、[Jammers]、[Generic - Frequency-Hopped]、[Generic - Continuous] があります。
Type	干渉のタイプを示します。クリックすると、種類の説明のポップアップにアクセスできます。
Status	アクティブまたは非アクティブを示します。 • [Active]：干渉源が現在 Spectrum Expert で検出されていることを示します。 • [Inactive]：Spectrum Expert が干渉を検出できなくなった、または干渉を確認した Spectrum Expert に Prime Infrastructure が到達できなくなったことを示します。
Discover Time	検出時刻を示します。
Affected Channels	影響を受けるチャネルを示します。
Number of APs Affected	次の条件を満たす場合、アクセスポイントは [Affected] としてリストされます。 • アクセス ポイントが Prime Infrastructure によって管理されている。 • Spectrum Expect がアクセス ポイントを検出している。 • Spectrum Expect がアクセス ポイントの稼働チャネル上の干渉源を検出している。
Power	dBm 単位で示されます。
Duty Cycle	% で示されます。100 % は最悪値を示します。
Severity	干渉の重大度ランキングを示します。100 % は最悪値を示し、0 は干渉源がないことを示します。

[Spectrum Experts Details] ページ

[Spectrum Expert Details] ページには、単一の Spectrum Expert からの干渉源の詳細がすべて表示されます。このページは 20 秒ごとに更新され、リモート Spectrum Expert の状況がリアルタイムに表示されます。次の項目が含まれています。

表 1-49　[Spectrum Experts Details] のフィールド

フィールド	説明
Total Interferer Count	特定の Spectrum Expert によって確認。
Active Interferers Count Chart	カテゴリ別に干渉をグループ化する円グラフを表示します。
Active Interferer Count Per Channel	異なるチャネルのカテゴリ別にグループ化した干渉の数を表示します。
AP List	Spectrum Expert がアクティブな干渉を検出したチャネル上で Spectrum Expert が検出したアクセス ポイントのリストを表示します。
Affected Clients List	現在認証されているか、またはアクセス ポイント リストにリストされたアクセス ポイントのいずれかの無線に関連付けられているクライアントのリストを表示します。

[Monitor] > [Network Devices] > [Wireless Controller] > [System Summary]

表 1-50 で、[Monitor] > [Network Devices] > [Wireless Controller] > [System Summary] の各フィールドについて説明します。

表 1-50　[Monitoring System Summary] ページのフィールド

フィールド	説明
General	
IP Address	コントローラ管理インターフェイスのローカル ネットワーク IP アドレス。
Name	ユーザ定義のコントローラ名。
Device Type	コントローラの種類。
UP Time	最後のリブートからの経過時間（日数、時間、および分単位）。
System Time	コントローラによって使用された時間。
Location	コントローラのユーザ定義された物理的な位置。
Contact	コントローラの担当者または所有者。
Total Client Count	現在コントローラにアソシエートされているクライアントの総数。
Current CAPWAP Transport Mode	Control And Provisioning of Wireless Access Points（CAPWAP）プロトコルのトランスポート モード。コントローラとアクセス ポイント間の通信です。[Layer 2] または [Layer 3] を選択します。
Power Supply One	電源が使用でき動作しているかどうか。これは 4400 シリーズ コントローラ専用です。

表 1-50　[Monitoring System Summary] ページのフィールド（続き）

フィールド	説明
Power Supply Two	電源が使用でき動作しているかどうか。これは 4400 シリーズ コントローラ専用です。
Inventory	
Software Version	現在コントローラで実行されているコードのオペレーティング システムの release.version.dot.maintenance 番号。
Emergency Image Version	コントローラのイメージ バージョン。
Description	インベントリ項目の説明。
Model No	Vital Product Data で定義されたマシン モデル。
Serial No	このコントローラの一意のシリアル番号。
Burned-in MAC Address	このコントローラのバーンドイン MAC アドレス。
Number of APs Supported	コントローラでサポートされているアクセス ポイントの最大数。
Gig Ethernet/Fiber Card	オプションの 1000BASE-T/1000BASE-SX GigE カードの有無を示します。
Crypto Card One	IPsec セキュリティを有効にして拡張処理能力を提供する、拡張セキュリティ モジュールの有無を示します。 **注**　デフォルトでは、拡張セキュリティ モジュールはコントローラに装着されていません。 Cisco Wireless LAN Controller に装着できる Crypto カードの最大数。 – Cisco 2000 シリーズ:なし – Cisco 4100 シリーズ:1 – Cisco 4400 シリーズ:2
Crypto Card Two	2 番めの拡張セキュリティ モジュールの有無を示します。
GIGE Port(s) Status	Up または Down。ポートのステータスを確認するにはクリックします。
Unique Device Identifier (UDI)	
Name	製品の種類。コントローラの場合は Chassis、アクセス ポイントの場合は Cisco AP。
Description	アクセス ポイントの数など、コントローラの説明。
Product ID	注文可能な製品 ID。
Version ID	製品 ID のバージョン。
Serial No	一意の製品シリアル番号。
Utilization	
CPU Utilization	指定した期間の最大、平均、および最小 CPU 使用率のグラフが表示されます。
Memory Utilization	指定した期間の最大、平均、および最小メモリ使用率のグラフが表示されます。

表 1-50　[Monitoring System Summary] ページのフィールド（続き）

フィールド	説明
Peer Memory Utilization	指定された期間の最大、平均、最小のピア メモリ使用率のグラフを表示します。
Peer CPU Usage for Standby Controller	指定された期間の最大、平均、最小のピア CPU 使用率のグラフを表示します。

[Wireless Controller] > [System] > [Spanning Tree Protocol]

表 1-51 で、[Monitor] > [Network Devices] > [Wireless Controller] > [Spanning Tree Protocol] の各フィールドについて説明します。

表 1-51　[Monitor] > [Network Devices] > [Wireless Controller] > [Spanning Tree Protocol] のフィールド

フィールド	説明
General	
Spanning Tree Specification	実行しているスパニング ツリー プロトコルのバージョン。IEEE 802.1D の実装は「IEEE 802.1D」を返します。現在のバージョンと互換性がない、将来のバージョンの IEEE スパニング ツリー プロトコルがリリースされた場合に、新しい値が定義されます。
Spanning Tree Algorithm	このコントローラがスパニング ツリー プロトコルに参加するかどうかを指定します。ドロップダウン リストで対応する行を選択することで有効または無効にできます。工場出荷時のデフォルトは無効です。
Priority	ブリッジ ID の書き込み可能な部分の値、つまり、ブリッジ ID の最初の 2 つのオクテット（8 オクテット長）です。ブリッジ ID の残りの（後半の）6 オクテットは、ブリッジの MAC アドレスの値によって設定されます。この値には 0 ～ 65535 の数値を指定できます。工場出荷時のデフォルトは 32768 です。
STP Statistics	
Topology Change Count	管理エンティティが最後にリセット、または初期化されてから、このブリッジによって検知されたトポロジに対する変更の総数。
Time Since Topology Changed	ブリッジによりトポロジの変更が検知されてから経過した時間（単位は日、時、分、秒）。
Designated Root	このノードで実行されているスパニング ツリー プロトコルによって決定される、スパニング ツリーのルートのブリッジ ID。この値は、このノードを起点とするコンフィギュレーション BPDU のすべての Root Identifier パラメータとして使用されます。
Root Cost	このブリッジからルートへのパスのコスト。
Root Port	このブリッジからルート ブリッジへの最も低いコスト パスを提供するポートのポート番号。

表 1-51　[Monitor] > [Network Devices] > [Wireless Controller] > [Spanning Tree Protocol] のフィールド（続き）

フィールド	説明
Maximum Age (seconds)	このブリッジがルートとして機能する場合、すべてのブリッジが MaxAge に使用する値。 **注**　802.1D-1990 によって、このパラメータの範囲は STP ブリッジのハロー タイムの値に関連することが規定されています。このタイマーの粒度は、802.1D-1990 によって 1 秒に規定されています。有効な値は 6 ～ 40 秒です。工場出荷時のデフォルトは 20 です。
Hello Time (seconds)	このブリッジがルートとして機能する場合、すべてのブリッジが HelloTime に使用する値です。このタイマーの粒度は、802.1D- 1990 によって 1 秒に規定されています。有効な値は 1 ～ 10 秒です。工場出荷時のデフォルトは 2 です。
Forward Delay (seconds)	このブリッジがルートとして機能する場合、すべてのブリッジが ForwardDelay に使用する値です。802.1D-1990 によって、このパラメータの範囲は STP ブリッジの最大経過時間の値に関連することが規定されています。このタイマーの粒度は、802.1D- 1990 によって 1 秒に指定されています。整数秒でない値を設定しようとした場合、エージェントによって badValue エラーが返されることがあります。有効な値は 4 ～ 30 秒です。工場出荷時のデフォルトは 15 です。
Hold Time seconds	特定の LAN ポートを通じたコンフィギュレーション BPDU の送信の間の最小経過時間。Hold Time 期間内に、多くても 1 個のコンフィギュレーション BPDU を送信します。

[Wireless Controller] > [System] > [CLI Sessions]

表 1-52 で、[Monitor] > [Network Devices] > [Wireless Controller] > [CLI Sessions] の各フィールドについて説明します。

表 1-52　[Monitor] > [Network Devices] > [Wireless Controller] > [CLI Sessions] のフィールド

フィールド	説明
Session Index	セッション ID。
Username	ログイン ユーザ名。
Connection Type	Telnet またはシリアル セッション。
Connection From	クライアント コンピュータ システムの IP アドレス。
Session Time	経過したアクティブ セッション時間。
Idle Time	経過した非アクティブ セッション時間。

[Wireless Controller] > [System] > [DHCP Statistics]

表 1-53 で、[Monitor] > [Network Devices] > [Wireless Controller] > [DHCP Statistics] の各フィールドについて説明します。

表 1-53　[Monitor] > [Network Devices] > [Wireless Controller] > [DHCP Statistics] のフィールド

フィールド	説明
Server IP	サーバの IP アドレスが示されます。
Is Proxy	このサーバがプロキシかどうかが示されます。
Discover Packets Sent	使用可能なサーバの場所を特定するために送信されたパケット数の合計が示されます。
Request Packets Sent	サーバのクライアントの要求パラメータから送信されたパケット数、またはアドレスの正当性を確認するために送信されたパケット数の合計が示されます。
Decline Packets	ネットワーク アドレスがすでに使用中であることを示すパケットの数が示されます。
Inform Packets	クライアントにはすでに外部でネットワーク アドレスが設定されており、そのクライアントから DHCP サーバへのローカル設定パラメータ要求の数を示します。
Release Packets	ネットワーク アドレスをリリースし、残りのリースをキャンセルするパケット数が示されます。
Reply Packets	応答パケット数が示されます。
Offer Packets	検出パケットに応答し、設定パラメータを提示するパケットの数が示されます。
Ack Packets	正常に送信されたことを知らせるパケットの数が示されます。
Nak Packets	送信でエラーが発生したことを知らせるパケット数が示されます。
Tx Failures	発生した転送エラーの数が示されます。
Last Response Received	最後に受け取った応答のタイムスタンプ。
Last Request Sent	最後に送信した要求のタイムスタンプ。

[Wireless Controller] > [WLANs]

表 1-54 で、[Monitor] > [Network Devices] > [Wireless Controller] > [WLAN] ページにあるフィールドについて説明します。

表 1-54　[Monitor] > [Network Devices] > [Wireless Controller] > [WLAN] のフィールド

フィールド	説明
WLAN ID	WLAN の識別番号。
Profile Name	最初に WLAN を作成するときに指定したユーザ定義プロファイル名。プロファイル名は WLAN 名です。
SSID	ユーザ定義の SSID 名。
Security Policies	WLAN で有効になっているセキュリティ ポリシー。
No of Mobility Anchors	モビリティ アンカーは、WLAN のアンカー コントローラとして指定されるモビリティ グループのサブセットです。
Admin Status	WLAN のステータスは有効または無効のいずれかです。
No. of Clients	この WLAN に現在アソシエートされているクライアントの数。

[Wireless Controller] > [Ports]

表 1-55 で、[Monitor] > [Network Devices] > [Wireless Controller] > [Physical Ports] ページにあるフィールドについて説明します。

表 1-55　[Monitor] > [Network Devices] > [Wireless Controller] > [Physical Ports] のフィールド

フィールド	説明
Port	ポートの詳細を表示するには、ポート番号をクリックします。
Physical Mode	すべてのポートの物理モードが表示されます。次の選択肢があります。 – 100 Mbps Full Duplex – 100 Mbps Half Duplex – 10 Mbps Full Duplex – 10 Mbps Half Duplex
Admin Status	ポートの状態が Enable または Disable で表示されます。
STP State	ポートの STP の状態が Forwarding または Disabled で表示されます。
Physical Status	実際のポートの物理インターフェイスが、次のいずれかで表示されます。 – Auto Negotiate – Half Duplex 10 Mbps – Full Duplex 10 Mbps – Half Duplex 100 Mbps – Full Duplex 100 Mbps – Full Duplex 1 Gbps
Link Status	赤（ダウン/障害）、黄（アラーム）、緑（アップ/正常）。

[Wireless Controller] > [CDP Neighbors]

表 1-56 で、[Monitor] > [Network Devices] > [Wireless Controller] > [CDP Neighbors] ページにあるフィールドについて説明します。

表 1-56　[Monitor] > [Network Devices] > [Wireless Controller] > [CDP Neighbors] のフィールド

フィールド	説明
Local Interface	ローカル ポート情報。
Neighbor Name	各 CDP ネイバーの名前。
Neighbor Address	各 CDP ネイバーの IP アドレス。
Neighbor Port	CDP パケットを送信するために各 CDP ネイバーが使用するポート。
Capability	各 CDP ネイバーの機能。
Platform	各 CDP ネイバー デバイスのハードウェア プラットフォーム。
Duplex	全二重または半二重を表示します。
Software Version	CDP ネイバーで実行されているソフトウェア。

[Wireless Controller] > [Security] > [RADIUS Authentication]

表 1-57 で、[Monitor] > [Network Devices] > [Wireless Controller] > [Security] > [RADIUS Authentication] ページにあるフィールドについて説明します。

表 1-57　[Monitor] > [Network Devices] > [Wireless Controller] > [Security] > [RADIUS Authentication] のフィールド

フィールド	説明
RADIUS Authentication Servers	
Server Index	RADIUS サーバのプライオリティ番号にアクセスします。最大 4 台のサーバを設定でき、サーバのコントローラによるポーリングはインデックス 1 で始まり、次にインデックス 2 というようになります。インデックス番号は、RADIUS サーバをコントローラに追加した順番で決まります。
IP Address	RADIUS サーバの IP アドレス。
ping	アイコンをクリックすると、コントローラから RADIUS サーバに ping が実行され、リンクが確認されます。
Port	インターフェイス プロトコルのコントローラのポート番号。
Admin Status	サーバが有効であるか無効であるかを示します。
Authentication Server Statistics	
Msg Round Trip Time	この RADIUS 認証サーバからの、最新の Access-Reply/Access-Challenge と、それに一致した Access-Request の間の間隔（ミリ秒単位）。
First Requests	このサーバに送信された RADIUS Access-Request パケットの数。再送信は含みません。
Retry Requests	この RADIUS 認証サーバに再送信された RADIUS Authentication-Request パケットの数。
Accept Responses	このサーバから受信した RADIUS Access-Accept パケットの数（有効または無効）。
Reject Responses	このサーバから受信した RADIUS Access-Reject パケットの数（有効または無効）。
Challenge Responses	このサーバから受信した RADIUS Access-Challenge パケットの数（有効または無効）。
Malformed Msgs	このサーバから受信した不正な形式の RADIUS Access-Response パケットの数。不正な形式のパケットには、長さが不正なパケットが含まれます。オーセンティケータまたはシグニチャ属性の不正や不明なタイプは、不正な形式のアクセス応答に含まれません。
Pending Requests	このサーバ宛の、まだタイムアウトしていないか、応答を受信していない RADIUS Access-Request パケットの数。この変数は、Access-Request を送信したときに増加し、Access-Accept、Access-Reject、または Access-Challenge の受信か、タイムアウトまたは再送信により減少します。
Bad Authentication Msgs	不正なオーセンティケータまたはシグニチャ属性が含まれた、このサーバから受信した RADIUS Access-Response パケットの数。
Timeouts Requests	このサーバに対する認証タイムアウトの数。タイムアウト後、クライアントは同じサーバに再試行するか、異なるサーバに送信するか、あきらめる可能性があります。同じサーバへの再試行は、再送信およびタイムアウトとしてカウントされます。異なるサーバへの送信は、要求およびタイムアウトとしてカウントされます。

表 1-57　[Monitor] > [Network Devices] > [Wireless Controller] > [Security] > [RADIUS Authentication] のフィールド（続き）

フィールド	説明
Unknown Type Msgs	このサーバから認証ポート上で受信した不明なタイプの RADIUS パケットの数。
Other Drops	このサーバから認証ポート上で受信し、他の何らかの理由でドロップされた RADIUS パケットの数。

[Wireless Controller] > [Security] > [RADIUS Accounting]

表 1-58 で、[Monitor] > [Network Devices] > [Wireless Controller] > [Security] > [RADIUS Accounting] ページにあるフィールドについて説明します。

表 1-58　[Monitor] > [Network Devices] > [Wireless Controller] > [Security] > [RADIUS Accounting] のフィールド

フィールド	説明
RADIUS Accounting Server	
Server Index	RADIUS サーバのプライオリティ番号にアクセスします。最大 4 台のサーバを設定でき、サーバのコントローラによるポーリングはインデックス 1 で始まり、次にインデックス 2 というようになります。インデックス番号は、RADIUS サーバをコントローラに追加した順番で決まります。
IP Address	RADIUS サーバの IP アドレス。
ping	アイコンをクリックすると、コントローラから RADIUS サーバに ping が実行され、リンクが確認されます。
Port	RADIUS サーバのポート。
Admin Status	サーバが有効であるか無効であるかを示します。
Accounting Statistics	
Msg Round Trip Time	この RADIUS アカウンティングサーバからの、最新の Accounting-Response とそれに一致した Accounting-Request の間の時間（ミリ秒単位）。
First Requests	送信した RADIUS Accounting-Request パケットの数。再送信は含みません。
Retry Requests	この RADIUS アカウンティング サーバに再送信された RADIUS Accounting-Request パケットの数。再送信には、Identifier と Acct-Delay が更新された再試行と、それらが同じ再試行が含まれます。
Accounting Responses	このサーバからアカウンティング ポートで受信した RADIUS パケットの数。
Malformed Msgs	このサーバから受信した不正な形式の RADIUS Accounting-Response パケットの数。不正な形式のパケットには、長さが不正なパケットが含まれます。オーセンティケータの不正や不明なタイプは、不正な形式のアカウンティング応答に含まれません。
Bad Authentication Msgs	このサーバから受信した、無効なオーセンティケータが含まれる RADIUS Accounting-Response パケットの数。
Pending Requests	このサーバに送信した、まだタイムアウトしていないか、応答を受信していない RADIUS Accounting-Request パケットの数。この変数は、Accounting-Request を送信したときに増加し、Accounting-Response の受信か、タイムアウトまたは再送信により減少します。

表 1-58　[Monitor] > [Network Devices] > [Wireless Controller] > [Security] > [RADIUS Accounting] のフィールド（続き）

フィールド	説明
Timeouts Requests	このサーバに対するアカウンティング タイムアウトの数。タイムアウト後、クライアントは同じサーバに再試行するか、異なるサーバに送信するか、あきらめる可能性があります。同じサーバへの再試行は、再送信およびタイムアウトとしてカウントされます。異なるサーバへの送信は、Accounting-Request およびタイムアウトとしてカウントされます。
Unknown Type Msgs	このサーバからアカウンティング ポート上で受信した不明なタイプの RADIUS パケットの数。
Other Drops	このサーバからアカウンティング ポート上で受信し、他の何らかの理由でドロップされた RADIUS パケットの数。

[Wireless Controller] > [Security] > [Management Frame Protection]

表 1-59 で、[Monitor] > [Network Devices] > [Wireless Controller] > [Security] > [Management Frame Protection] ページにあるフィールドについて説明します。

表 1-59　[Monitor] > [Network Devices] > [Wireless Controller] > [Security] > [Management Frame Protection] のフィールド

フィールド	説明
General	
Management Frame Protection	コントローラでインフラストラクチャ MFP がグローバルに有効になっているかどうかを示します。
Controller Time Source Valid	[Controller Time Source Valid] フィールドには、コントローラ時間がローカルに設定されたか（手動で時刻を入力）、または外部ソース（NTP サーバなど）を通じて設定されたかを示します。時刻が外部ソースによって設定される場合は、このフィールドの値が "True" になります。時刻がローカルに設定される場合は、この値が "False" になります。時刻源は、モビリティ グループ内の複数のコントローラのアクセス ポイント間の管理フレーム上のタイムスタンプを検証するために使用されます。
WLAN Details	
WLAN ID	WLAN ID。1 ～ 17。
WLAN Name	最初に WLAN を作成するときに指定したユーザ定義プロファイル名。SSID 名とプロファイル名の両方がユーザ定義です。WLAN 名はプロファイル名と同じです。
MFP Protection	管理フレーム保護は、有効または無効のいずれかです。
Status	WLAN のステータスは有効または無効のいずれかです。
AP Details	
AP Name	オペレータが定義したアクセス ポイント名。
MFP Validation	管理フレーム保護は、有効または無効のいずれかです。
Radio	802.11a または 802.11b/g。
Operation Status	動作ステータス（UP または DOWN）が表示されます。

表 1-59　[Monitor] > [Network Devices] > [Wireless Controller] > [Security] > [Management Frame Protection] のフィールド（続き）

フィールド	説明
Protection	Full（全フレーム）。
Validation	Full（全フレーム）。

[Wireless Controller] > [Security] > [Rogue AP Rules]

表 1-60 で、[Monitor] > [Network Devices] > [Wireless Controller] > [Security] > [Rogue AP Rules] ページにあるフィールドについて説明します。

表 1-60　[Monitor] > [Network Devices] > [Wireless Controller] > [Security] > [Rogue AP Rules] のフィールド

フィールド	説明
Rule Name	ルールの名前。
Rule Type	Malicious または Friendly • [Malicious Rogue]：検出されたアクセス ポイントのうち、ユーザが定義した Malicious ルールに一致したアクセス ポイント、または危険性のない AP カテゴリから手動で移動されたアクセス ポイント。 • [Friendly Rogue]：既知、認識済み、または信頼できるアクセス ポイント、または検出されたアクセス ポイントのうち、ユーザが定義した Friendly ルールに該当するアクセス ポイント。
Match Type	match any または match all 条件。
Enabled Rule Conditions	有効なすべてのルール条件を示します。次のものが含まれます。 • Open Authentication • Match Managed AP SSID • Match User Configured SSID • Minimum RSSI • Time Duration • Minimum Number Rogue Clients

[Wireless Controller] > [Security] > [Guest Users]

表 1-61 で、[Monitor] > [Network Devices] > [Wireless Controller] > [Security] > [Guest Users] ページにあるフィールドについて説明します。

表 1-61　[Monitor] > [Network Devices] > [Wireless Controller] > [Security] > [Guest Users] のフィールド

フィールド	説明
Guest User Name	ゲスト ユーザのログイン名を示します。
Profile	ゲスト ユーザが結びつけられているプロファイルを示します。
Lifetime	ゲスト ユーザ アカウントがアクティブな時間の長さを示します。時間の長さは、日、時間、分単位で表示されるか、Never Expires と表示されます。

表 1-61　[Monitor] > [Network Devices] > [Wireless Controller] > [Security] > [Guest Users] のフィールド（続き）

フィールド	説明
Start Time	ゲスト ユーザ アカウントがアクティブ化された時刻を示します。
Remaining Lifetime	ゲスト ユーザ アカウントの残り時間を示します。
Role	指定されたユーザ ロールを示します。
First Logged in at	ユーザが最初にログインした日付と時刻を示します。
Number of logins	このゲスト ユーザの合計ログイン回数を示します。
Description	識別を目的とする、ゲスト ユーザ アカウントのユーザ定義の説明です。

[Wireless Controller] > [Mobility] > [Mobility Stats]

表 1-60 で、[Monitor] > [Network Devices] > [Wireless Controller] > [Mobility] > [Mobility Stats] ページにあるフィールドについて説明します。

表 1-62　[Monitor] > [Network Devices] > [Wireless Controller] > [Mobility] > [Mobility Stats] のフィールド

フィールド	説明
Global Mobility Statistics	
Rx Errors	短すぎるパケットや不正な形式などの、一般的なプロトコル パケット受信エラー。
Tx Errors	パケット送信失敗など、一般的なプロトコル パケット送信エラー。
Responses Retransmitted	モビリティ プロトコルは UDP を使用し、応答が受信されない場合には、複数回にわたって要求が再送信されます。ネットワークの遅延または処理の遅延のため、応答側が最初に要求に応答した後に、1 回以上の再試行要求を受信する場合があります。このフィールドは、応答が再送信された回数です。
Handoff Requests Received	ハンドオフ要求が受信、無視または応答された合計回数。
Handoff End Requests	ハンドオフ終了要求が受信された合計回数。これらの要求は、クライアント セッションの終了について相手に通知するために、アンカー コントローラまたは外部コントローラによって送信されます。
State Transitions Disallowed	PEM（ポリシー施行モジュール）がクライアントのステート遷移を拒否しました。通常、その結果としてハンドオフが中断されます。
Resource Unavailable	バッファなどの必要なリソースが使用できませんでした。その結果としてハンドオフが中断されます。
Mobility Responder Statistics	
Handoff Requests Ignored	無視されたハンドオフ要求またはクライアント通知の数。コントローラには、単にそのクライアントに関する知識がありません。
Ping Pong Handoff Requests Dropped	ハンドオフ期間が短すぎた（3 秒）ために拒否されたハンドオフ要求の数。
Handoff Requests Dropped	クライアントについての認識が不完全であるか、パケットの問題が原因でドロップされたハンドオフ要求の数。
Handoff Requests Denied	積極的に拒否されたハンドオフ要求の数。
Client Handoff as Local	ローカル ロール中に送信されたハンドオフ応答の数。
Client Handoff as Foreign	外部ロール中に送信されたハンドオフ応答の数。
Anchor Requests Received	受信したアンカー要求の数。

表 1-62　[Monitor] > [Network Devices] > [Wireless Controller] > [Mobility] > [Mobility Stats] のフィールド（続き）

フィールド	説明
Anchor Requests Denied	拒否されたアンカー要求の数。
Anchor Requests Granted	許可されたアンカー要求の数。
Anchor Transferred	クライアントが外部コントローラから現在のアンカーと同じサブネット上のコントローラに移動したために、転送されたアンカーの数。
Mobility Initiator Statistics	
Handoff Requests Sent	コントローラにアソシエートされ、モビリティ グループに通知されたクライアントの数。
Handoff Replies Received	送信された要求に応答して受信された、ハンドオフ応答の数。
Handoff as Local Received	クライアント セッション全体が転送されたハンドオフの数。
Handoff as Foreign Received	クライアント セッションが別の場所でアンカーされたハンドオフの数。
Handoff Denies Received	拒否されたハンドオフの数。
Anchor Request Sent	スリーパーティ(外部から外部)ハンドオフ用に送信されたアンカー要求の数。ハンドオフが別の外部コントローラから受信され、新しいコントローラがクライアントを移動させるようアンカーに要求しています。
Anchor Deny Received	現在のアンカーによって拒否されたアンカー要求の数。
Anchor Grant Received	現在のアンカーによって許可されたアンカー要求の数。
Anchor Transfer Received	現在のアンカーによって受信されたアンカー転送の数。

[Wireless Controller] > [Redundancy] > [Redundancy Summary]

表 1-60 で、[Monitor] > [Network Devices] > [Wireless Controller] > [Redundancy] > [Redundancy Summary] ページにあるフィールドについて説明します。

表 1-63　[Monitor] > [Network Devices] > [Wireless Controller] > [Redundancy] > [Redundancy Summary] のフィールド

フィールド	説明
Local State	ステータスを表示します。
Peer State	ピアの状態情報を表示します。
Active Controller	アクティブなコントローラがプライマリ コントローラかセカンダリ コントローラかを表示します。
Unit Mac	ユニットの MAC アドレスを表示します。
Redundancy State	冗長性状態を表示します。
Mobility MAC	モビリティ MAC アドレス。
Redundancy-Management IP	冗長性管理 IP アドレス。
Peer Redundancy-Management IP	ピア冗長性管理 IP アドレス情報。
Redundancy port IP	冗長性ポート IP アドレス。
Peer Redundancy port IP	ピア冗長性ポート IP アドレス。
Peer Service Port IP	ピア サービス ポートの IP アドレス。

表 1-63　[Monitor] > [Network Devices] > [Wireless Controller] > [Redundancy] > [Redundancy Summary] のフィールド（続き）

フィールド	説明
Average Redundancy Peer Reachability Latency (Micro seconds)	冗長性ピアの平均到達可能性遅延をマイクロ秒単位で表示します。
Average Management Gateway Reachability Latency (Micro seconds)	管理ゲートウェイに到達するまでの平均遅延をマイクロ秒単位で表示します。
Primary to Standby BulkSync Status	プライマリからスタンバイ コントローラへの設定同期のステータスを表示します。

[Monitor Tools]

次に、[Monitor Tools] フィールドについて説明します。

- [Packet Capture] > [Capture Sessions]（ 1-51 ページ）
- [Monitor] > [Wireless Technologies Tools]（ 1-52 ページ）

[Packet Capture] > [Capture Sessions]

次の表で、[Monitor] > [Tools] > [Packet Capture] > [Capture Sessions] .にあるフィールドについて説明します。

表 1-64　[Monitor] > [Tools] > [Packet Capture]

フィールド	説明
Name	このキャプチャ セッションの一意の名前を入力します。
Packet Slice Size (bytes)	パケット全体をキャプチャするには、0 を入力します。
File Size (MB)	キャプチャ ファイルの総サイズ。
Rotate Files	このオプションが有効になっている場合は、明示的に停止するまで、キャプチャは継続されます。 NAM の場合は、結果は「number of files」パラメータにより、ラウンド ロビン シーケンスに保存されます。例えば、「rotate」が真で、「number of files」が 2 の場合、2 つのキャプチャ ファイルが内容の保存に使用されます。パケットは、いっぱいになるまでは最初のファイルに保存され、次のファイルでそのプロセスが繰り返されます。 ASR の場合は、パケット ファイルが循環します（同じファイルが使用され、内容は上書きされます）。

表 1-64　[Monitor] > [Tools] > [Packet Capture]（続き）

フィールド	説明
For ASR devices only:	• [Packet-to-Sample]:*n* 番目のパケットをキャプチャします。例えば、「3」は、3 つ目のパケットごとという意味です。 • [Packet-Rate]:1 秒あたりにキャプチャするパケットの数（最小値:1、有効なエントリ:0 ～ 9）。 • [Duration]:キャプチャする時間。 • [Packets]:キャプチャするパケットの総数。
Number of files	内容の保存に使用するファイルの数。NAM デバイスの場合のみ。

[Monitor] > [Wireless Technologies Tools]

次に、[Monitor] > [Wireless Technologies Tools] にあるページの各フィールドについて説明します。

[Voice Audit] フィールドの説明

次の表で、[Monitor] > [Tools] > [Wireless Voice Audit] ページの各フィールドについて説明します。

- [Voice Audit] > [Controller] タブ（ 1-52 ページ）
- [Voice Audit] > [Rules] タブ（ 1-53 ページ）
- [Voice Audit] > [Report] タブ（ 1-56 ページ）

[Voice Audit] > [Controller] タブ

次の表で、[Monitor] > [Tools] > [Wireless Voice Audit] > [Controllers] の各フィールドについて説明します。

表 1-65　[Wireless Voice Audit] > [Controller] タブのフィールドの説明

フィールド	説明
Run audit on	次のいずれかのオプションを選択します。 • [All Controllers]:追加のコントローラ情報は不要です。 • [A Floor Area]:ドロップダウン リストから、該当するキャンパス、ビルディング、フロア、およびコントローラを選択します。 • [A Single Controller]:該当するコントローラをドロップダウン リストから選択します。

[Voice Audit] > [Rules] タブ

次の表で、[Monitor] > [Tools] > [Wireless Voice Audit] > [Rules] の各フィールドについて説明します。

表 1-66　[Wireless Voice Audit] > [Rules] タブのフィールドの説明

ルール	ルールの詳細
VoWLAN SSID	説明:VoWLAN SSID が存在するかどうかを確認します。 ルールの有効性:ユーザ定義の VoWLAN SSID。
CAC: 7920	説明:7920 AP CAC が VoWLAN で有効になっているかどうかを確認します。 ルールの有効性:ユーザ定義の VoWLAN SSID。
CAC: 7920 Clients	説明:7920 クライアント CAC が VoWLAN で無効になっているかどうかを確認します。 ルールの有効性:ユーザ定義の VoWLAN SSID。
DHCP Assignment	説明:DHCP の割り当てが VoWLAN で無効になっているかどうかを確認します。 ルールの有効性:ユーザ定義の VoWLAN SSID。
MFP Client	説明:VoWLAN で MFP クライアント保護が [Required] に設定されていないかどうかを確認します。 ルールの有効性:ユーザ定義の VoWLAN SSID。
Platinum QoS	説明:VoWLAN で QoS が Platinum(Voice)に設定されているかどうかを確認します。 ルールの有効性:ユーザ定義の VoWLAN SSID。
Non Platinum QoS	説明:非 VoWLAN で QoS が Platinum に設定されていないことを確認します。 ルールの有効性:ユーザ定義の VoWLAN SSID。
WMM	説明:WMM が VoWLAN で有効になっているかどうかを確認します。 ルール データ:ドロップダウン リストから [Allowed] または [Required] を選択します。 ルールの有効性:ユーザ定義の VoWLAN SSID。
CCKM	説明:CCKM が VoWLAN で有効になっているかどうかを確認します。 ルールの有効性:ユーザ定義の VoWLAN SSID。
CCKM With No AES- for 792x phones	説明:VoWLAN 向けの Cisco Centralized Key Management(CCKM)で AES 暗号化が有効になっていないことを確認します。このルールは、792x 電話機専用です。 ルールの有効性:ユーザ定義の VoWLAN SSID。
TSM	説明:Traffic Stream Metrics(TSM)が有効になっていることを確認します。 ルール データ:[802.11a/n TSM] または [802.11b/g/n TSM]、あるいは両方のチェックボックスをオンにします。 ルールの有効性:少なくとも 1 つのバンドを選択する必要があります。
DFS	説明:Channel Announcement と Channel Quite Mode の両方で、動的周波数選択(DFS)が有効になっているかどうかを確認します。

表 1-66　[Wireless Voice Audit] > [Rules] タブのフィールドの説明（続き）

ルール	ルールの詳細
ACM	説明:アドミッション制御が有効になっているかどうかを確認します。 ルール データ:[802.11a/n ACM] または [802.11b/g/n ACM]、あるいは両方のチェックボックスをオンにします。 ルールの有効性:少なくとも 1 つのバンドを選択する必要があります。
DTPC	説明:動的送信電力制御が有効になっているかどうかを確認します。 ルール データ:[802.11a/n DTPC] または [802.11b/g/n DTPC]、あるいは両方のチェックボックスをオンにします。 ルールの有効性:少なくとも 1 つのバンドを選択する必要があります。
Expedited Bandwidth	説明:緊急帯域幅が有効になっているかどうかを確認します。 ルール データ:[802.11a/n Expedited Bandwidth] または [802.11b/g/n Expedited Bandwidth]、あるいは両方のチェックボックスをオンにします。 ルールの有効性:少なくとも 1 つのバンドを選択する必要があります。
Load Based CAC	説明:負荷ベースのアドミッション制御(CAC)が有効になっているかどうかを確認します。 ルール データ:[802.11a/n Load Based CAC] と [802.11b/g/n Load Based CAC (LBCAC)] のいずれかまたは両方のチェックボックスをオンにします。 ルールの有効性:少なくとも 1 つのバンドを選択する必要があります。
CAC: Max Bandwidth	説明:コール アドミッション制御の最大 RF 帯域幅が適切に設定されているかどうかを確認します。 ルール データ:802.11a/n と 802.11b/g/n の最大許容帯域幅のテキスト ボックスにパーセンテージを入力します。 ルールの有効性:少なくとも 1 つの帯域のデータを指定する必要があります。有効な値の範囲は 0 ～ 100 % です。
CAC: Reserved Roaming Bandwidth	説明:コール アドミッション制御の予約済みローミング帯域幅が適切に設定されているかどうかを確認します。 ルール データ:テキスト ボックスに、802.11a/n と 802.11b/g/n の最大予約済みローミング帯域幅のパーセンテージを入力します。 ルールの有効性:少なくとも 1 つの帯域のデータを指定する必要があります。有効な値の範囲は 0 ～ 100 % です。
Pico Cell mode	説明:ピコ セル モードが無効になっているどうかを確認します。 ルール データ:[802.11a/n Pico Cell mode] と [802.11b/g/n Pico Cell mode] のいずれかまたは両方のチェックボックスをオンにします。 ルールの有効性:少なくとも 1 つのバンドを選択する必要があります。
Beacon Period	説明:ビーコン周期が適切に設定されているかどうかを確認します。 ルール データ:テキスト ボックスに、11a/n および 11b/g/n のビーコン周期(ミリ秒単位)を入力します。 ルールの有効性:少なくとも 1 つの帯域のデータを指定する必要があります。有効な範囲は 20 ～ 1000 です。0 を入力するか、帯域を確認しない場合は空欄のままにします。

表 1-66　[Wireless Voice Audit] > [Rules] タブのフィールドの説明（続き）

ルール	ルールの詳細
Short Preamble	説明:11b/g にショート プリアンブルが有効になっているかどうかを確認します。
Fragmentation Threshold	説明:フラグメンテーション閾値が適切に設定されているかどうかを確認します。 ルール データ:テキスト ボックスに、11a/n と 11b/g/n のフラグメンテーション閾値(バイト単位)を入力します。 ルールの有効性:少なくとも 1 つの帯域のデータを指定する必要があります。有効な範囲は 256 ～ 2346 です。0 を入力するか、帯域を確認しない場合は空欄のままにします。
Data Rate	説明:データ レートが適切に設定されているかどうかを確認します。 11b/g のデータ レート設定:各 Mbps カテゴリで、[Disabled] 、[Supported] 、または [Mandatory] を選択します。 11a のデータ レート設定:各 Mbps カテゴリで、[Disabled] 、[Supported] 、または [Mandatory] を選択します。
Aggressive Load Balancing	説明:アグレッシブ ロード バランシングが無効になっているかどうかを確認します。
QoS Profile	説明:QoS プロファイルがデフォルト値から変更されていないことを確認します。
EAP Request Timeout	説明:EAP 要求タイムアウトが適切に設定されているかどうかを確認します。 ルール データ:EAP 要求タイムアウトの時間制限(秒単位)を入力します。 ルールの有効性:データを空白のままにしたりゼロを設定したりできません。有効な範囲は 1 ～ 120 です。
ARP Unicast	説明:ARP ユニキャストが無効になっているどうかを確認します。

[Voice Audit] > [Report] タブ

次の表で、[Monitor] > [Tools] > [Wireless Voice Audit] > [Report] の各フィールドについて説明します。

表 1-67　[Wireless Voice Audit] > [Report] タブのフィールドの説明

フィールド	説明
Audit Status	監査が完了しているかどうかを示します。
Start Time and End Time	音声監査の開始時刻と終了時刻を示します。
# Total Devices	音声監査に関与するデバイスの数を示します。
# Completed Devices	ツールが監査しようとしたデバイスを数を示します。 **注**　コントローラが到達不能な場合、そのコントローラの監査がスキップされます。そのコントローラに対してはルール チェックが実行されません。
# Rules	音声監査に選択したルールの数を示します。
Report Results	
IP Address	音声監査に関与するコントローラの IP アドレスを示します。
Rule	このコントローラに適用されたルールを示します。
Result	適用されたルールの結果（[Skipped]、[Violation]、[Unreachable]）を示します。 **注**　現在の設定とルール値に不一致が存在しない場合、そのルールの結果は表示されません。
Details	ルールの結果の説明を定義します。 **注**　適用されたルールの結果が [Violation] である場合、[Details] リンクをクリックすると、名前、デバイス値、ルール値などの詳細が表示されます。リンクにマウス カーソルを合わせると詳細が表示されます。
Time	音声監査のタイプスタンプを指定します。

[Voice Diagnostic] フィールドの説明

次の表で、[Monitor] > [Tools] > [Wireless Voice Diagnostic] ページの各フィールドについて説明します。

- [Voice Diagnostic Test List] ページ（ 1-56 ページ）
- [Voice Diagnostic Test Report] ページ（ 1-57 ページ）

[Voice Diagnostic Test List] ページ

次の表で、[Monitor] > [Tools] > [Wireless Voice Diagnostic] の各フィールドについて説明します。

表 1-68　[Voice Diagnostic Test List] ページのフィールドの説明

フィールド	説明
Test Name	テストの名前。
Duration of Test (Minutes)	テストが実行される継続時間。継続時間は、10 分、20 分、30 分、40 分、50分、60 分のいずれかです。デフォルトの選択値は 10 分です。

表 1-68　[Voice Diagnostic Test List] ページのフィールドの説明（続き）

フィールド	説明
First Client	クライアントの MAC アドレスやそのクライアントにプロビジョニングされたすべてのコントローラなど、最初のクライアントの詳細情報を表示します。また、コントローラに到達できない場合は、プロビジョニングに失敗したコントローラもリストされます。
Second Client	クライアントの MAC アドレスやそのクライアントにプロビジョニングされたすべてのコントローラなど、2 番目のクライアントがある場合は、その詳細情報を表示します。また、コントローラに到達できない場合は、プロビジョニングに失敗したコントローラもリストされます。
Start Time	テストが開始された時刻。
Remaining Time	テストの残り時間。
State	テストの状態。[Running]、[Completed]、[Stopped]、または [Aborted] の 4 つの状態のいずれかです。
Problem	テストのステータス。赤はテストで問題が検出されたことを示します。緑色は、コール中の問題が検出されなかった音声診断テストを示します。

[Voice Diagnostic Test Report] ページ

次の表で、[Monitor] > [Tools] > [Wireless Voice Diagnostic Test Report] のタブについて説明します。

表 1-69　[Voice Diagnostic Test Report] ページのタブの説明

タブ	説明
概要	
このタブは、3 つの領域に分かれています。上部の領域にはテストとクライアントの詳細情報が表示されます。真ん中の領域には問題が表示され、下部の領域には対応するログ メッセージが表示されます。	
Test and Client Details	[Test Status] に、テストの名前、1 番めのクライアントの MAC アドレス、2 番めのクライアントの MAC アドレス、デバイス タイプ、テスト ステータス、開始時刻、残り時間、テスト期間などのテスト詳細が表示されます。テストが中断した場合、またはテストが完了した場合は再起動します。実行中のテストを停止する [Stop] ボタンが表示されます。ステータスおよびクライアントの詳細を更新するには、[Refresh Status Tab] ボタンおよび [Refresh Client Tab] ボタンを使用します。クライアントのユーザ名、IP アドレス、MAC アドレス、ベンダー、CCX バージョン、802.11 の状態、プロトコル、SSID、プロファイル名、AP の詳細など、クライアントの詳細情報が表示されます。クライアントの詳細情報を参照するには、クライアントの MAC アドレスをクリックします。
Problems	[Problems] ペインは [Test and Client Details] ペインの下に表示されます。このペインには、現在の診断に関するすべての問題が表示されます。このペインは 5 秒ごとに個別に更新されます。ページ全体を更新する必要はありません。このペインの情報をソートするには、ペインのいずれかの列をクリックします。[Problems] ペインの行をクリックすると、問題の詳しい説明と推奨アクションが示されたダイアログ ボックスが表示されます。 **注**　コントローラ間ローミングの障害の場合、[From AP information] 内の MAC アドレスが正確でなく、「00:00:00:00:00:00」と表示されることがあります。
Logs	[Logs] ペインは、[Problems] ペインの下に表示されます。このペインには、この診断中にコントローラと WCS 間でやり取りされたすべてのメッセージが表示されます。このペインの情報をソートするには、ペインのいずれかの列をクリックします。このペインは、ページ全体を更新しなくても、5 秒ごとに個別に更新されます。

表 1-69　[Voice Diagnostic Test Report] ページのタブの説明（続き）

タブ	説明
チャート	
このタブには、各クライアントのアップリンクおよびダウンリンク トラフィックのグラフが表示されます。チャートは 10 秒ごとに更新されます。	
Client Uplink and DownLink TSM Chart with Roaming	[Client Uplink Traffic Stream Metric (TSM)] チャートには、CCX V4 以上をサポートするクライアントが表示されます。TMS データは 10 秒ごとにプロットされます。TSM チャートには、一連のシリーズのメトリックが表示され、チャート内の [Select Series] ボタンを使用して有効または無効にできます。
Client Uplink and DownLink QoS Chart	間隔ごとに、QoS が計算され、[Client Uplink QoS] チャートを表すチャートに表示されます。この円グラフには、QoS チャートの総数と、3 つのカテゴリ内での分布が表示されます。これらのカテゴリは一般に、音声コールの品質を示します。
Average Uplink and Downlink AC Queue	[AC Queue] には、パケットのタイプと、シリーズのパケットの数が表示されます。[Select Series] ボタンを使用して、シリーズを有効または無効にできます。
Roam History	
このタブには、ローミング テーブル内のローミング履歴情報が表示されます。このローミング テーブルには、成功したローミング履歴と失敗したローミング履歴の両方が表示されます。ローミング テーブルでは、次の情報が提供されます。 • クライアントのローミングが実行された時刻 • クライアントの移動元の AP の名前 • クライアントの移動元の無線のタイプ • クライアントの移動元のコントローラの IP アドレス • クライアントの移動先の AP の名前 • クライアントの移動先のコントローラの IP アドレス • クライアントの移動先の無線のタイプ • ローミングの結果（成功したか失敗したか） • 失敗の場合は、その失敗の理由も表示されます。	
Event	
[Event] タブには、リスト内の音声コール時のクライアントと AP に関連するイベント履歴が表示されます。最後の 10 のイベントが表示されます。[Client Events] と [AP Events] の 2 つのイベント テーブルを利用できます。音声コール時のクライアント固有のイベントは [Client Events] テーブルに、AP 固有のイベントは [AP Event] テーブルに表示されます。	

[Monitor] > [WiFi TDOA Receivers]

次の表で、[Monitor] > [TDOA Receivers] ページの各フィールドについて説明します。

表 1-70　[Monitor] > [TDOA Receivers] フィールド

フィールド	説明
MAC Address	WiFi TDOA レシーバの MAC アドレス。
WiFi TDOA Receiver Name	TDOA レシーバの名前。

表 1-70　[Monitor] > [TDOA Receivers] フィールド（続き）

フィールド	説明
Static IP	WiFi TDOA レシーバのスタティック IP アドレス。
Oper Status	ステータスが [Up] か [Down] かを表示します。
Map Location	WiFi TDOA レシーバのフロア マップを表示するには、[Map Location] リンクをクリックします。

[Media Streams]

次に、[Media Streams] フィールドについて説明します。

- [Monitor] > [Media Streams]
- [Monitor] > [Media Streams] > [Media Stream Details]

[Monitor] > [Media Streams]

次の表で、[Monitor] > [Media Streams] ページの各フィールドについて説明します。

表 1-71　[Monitor] > [Media Streams] フィールド

フィールド	説明
Stream Name	メディア ストリームの名前。メディア ストリームの詳細情報を表示するには、[Stream Name] をクリックします。
Start IP	マルチキャスト ダイレクト機能が有効になっているメディア ストリームの開始 IP アドレス。
End IP	マルチキャスト ダイレクト機能が有効になっているメディア ストリームの終了 IP アドレス。
State	メディア ストリームの動作状態。
Max Bandwidth	メディア ストリームに割り当てられている最大帯域幅。
Priority	メディア ストリーム内に設定されているプライオリティ ビット。プライオリティは 1 ～ 8 の任意の数字です。値が小さいほど、プライオリティは高くなります。たとえば、プライオリティ 1 が最も高く、値 8 は最も低くなります。
Violation	違反が発生した場合に実行されるアクション。表示される値は次のとおりです。 • [Drop]：定期的な再評価時にストリームがドロップされることを示します。 • [Best Effort]：定期的な再評価時にストリームがベストエフォート クラスにデモートされることを示します。
Policy	メディア ストリーム ポリシー。取り得る値は [Admit] または [Deny] です。
Controllers	指定したメディア ストリームを使用するコントローラの数。
Clients	指定したメディア ストリームを使用するクライアントの数。

[Monitor] > [Media Streams] > [Media Stream Details]

次の表で、[Monitor] > [Media Streams] > [Media Stream Details] ページの各フィールドについて説明します。

表 1-72　[Monitor] > [Media Streams] > [Media Stream Details] のフィールド

フィールド	説明
Media Stream Details	次のメディア ストリーム設定情報を表示します。 • Media Stream Name • Multicast Destination Start IP • Multicast Destination End IP • Maximum Expected Bandwidth (1 to 35000 kbps) • Operational Status • Average Packet Size(100-1500 bytes) • RRC Periodic • RRC Priority(1-8) • Traffic Profile Violation • Policy
Statistics	選択したメディア ストリームを使用するコントローラの数とクライアントの数を表示します。コントローラ数をクリックすると、選択したメディア ストリームを使用するコントローラの一覧にアクセスできます。
Error	その AP のエラーと対応するフロア マップを表示します。
Client Counts	各期間のクライアントの数を表示します。クライアント情報は、時間ベースのグラフに表示されます。時間ベースのグラフでは、グラフ ページの上部に、6 時間、1 日、1 週間、2 週間、4 週間、3 ヵ月、6 ヵ月、1 年、およびカスタムを表示するリンク バーがあります。選択すると、そのタイム フレームのデータが取得され、対応するグラフが表示されます。
Failed Client Counts	各期間の失敗したクライアントの数を表示します。

関連項目

- Configuring Wi-Fi TDOA Receivers
- Adding Wi-Fi TDOA Receivers to the Prime Infrastructure Database
- Positioning Wi-Fi TDOA Receivers

[Monitor] > [Radio Resource Management]

次の表で、[Monitor] > [Radio Resource Management] ページの各フィールドについて説明します。

表 1-73　[Monitor] > [Radio Resource Management] のフィールド

フィールド	説明
RRM Statistics	次のネットワーク全体の RRM パフォーマンスの統計情報を表示し、まとめてグループ化したイベントに基づいてチャネル変更の理由を予測します。 • [Number of RF Groups]：Prime Infrastructure が現在管理している RF グループの総数を表示します。 • [APs at maximum power (a/n/ac)]：802.11 a/n 無線によるアクセス ポイントが最大電力であった時間の割合を表示し、それらのアクセス ポイントの場所を示します。 • [APs at maximum power (b/g/n)]：802.11 a/n 無線によるアクセス ポイントが最大電力であった時間の割合を表示し、それらのアクセス ポイントの場所を示します。 • [Total Configuration Mismatches]：24 時間にわたって検出された設定不一致の総数を表示します。 • [Total Channel Changes]：チャネルが更新されたか、改訂されたかにかかわらず、802.11a/b/g/n 無線でのチャネル変更の総数を表示します。カウントは、24 時間および 7 日間の期間に分割されます。割合のリンクまたは [24-hour] 列の下にあるリンクをクリックすると、そのアクセス ポイントのみの詳細を示すページが表示されます。 • [CleanAir Initiated Channel Changes]：CleanAir により開始されたチャネル変更情報を表示します。 • [Total Coverage Hole Events]：7 日間、1 日 24 時間にわたるカバレッジ ホール イベントの総数を表示します。
Channel Change Reason	すべての 802.11a/b/g/n 無線についてチャネルが変更された理由を表示します。次のパラメータが含まれています。 • 信号：他のいくつかの近隣する無線のチャネル品質が改善されたためにチャネルが変更されました。他のネイバー無線のチャネル品質を向上させると、アルゴリズムで評価されたように、システムのチャネル計画が向上しました。 • WiFi 干渉 • 負荷 • レーダー • ノイズ • Persistent Non-Wifi interference • 主要な電波品質イベント • Other

表 1-73　[Monitor] > [Radio Resource Management] のフィールド（続き）

フィールド	説明
Channel Change Causes	802.11a/n 無線のグラフィカルな横棒グラフを表示します。グラフは、チャネル変更が行われた理由に基づいて作成されます。グラフは 2 つの部分に分割され、それぞれ 24 時間および 7 日間に発生するイベントを引き起こす理由の重み付けされた理由の割合を示します。チャネル変更の各イベントにはいくつかの理由があり、その重みはそれらの理由に均等に分けられます。ネット原因コードは、イベントが発生した理由の数に関係なく、1 という係数が与えられます。
Channel Change - APs with channel changes	チャネル変更情報を表示します。チャネル変更の各イベントには、Lightweight アクセス ポイントの MAC アドレスが含まれます。各理由コードについて、チャネル イベントの重み付き理由に基づいて 802.11a/n アクセス ポイントに発生したチャネル変更の多くが表示されます。カウントは、24 時間および 7 日間の期間に分割されます。
Configuration Mismatch - RF Groups with Configuration Mismatches	24 時間にわたる設定不一致を RF グループの詳細情報別に表示します。
Coverage Hole - APs reporting coverage holes	カバレッジ ホール イベントをトリガーした（しきい値ベース）IF Type 11 a/n によってフィルタリングされた上位 5 つのアクセス ポイントを表示します。
APs at Maximum Power	カバレッジ ホール イベントに対応するため最大電力で動作している 802.11a/n Lightweight アクセス ポイントの合計のパーセンテージのグラフィカルなプログレッシブ チャートを表示します。カウントは、24 時間および 7 日間の期間に分割されます。

[Alarms and Events]

次に、[Alarms and Events] の各フィールドについて説明します。

- [Monitoring Tools] > [Alarms and Events] > [Alarms] タブ
- [Monitor] > [Monitoring Tools] > [Clients and Users]

[Monitoring Tools] > [Alarms and Events] > [Alarms] タブ

次の表で、[Monitor] > [Monitoring Tools] > [Alarms and Events] > [Alarms] タブの各フィールドについて説明します。

表 1-74　[Monitor] > [Monitoring Tools] > [Alarms and Events] > [Alarms] タブのフィールド

フィールド	説明
Severity	次のいずれかのアラームの重大度。 • Critical • Major • Minor • Warning • Informational
Message	アラームについてのメッセージ

表 1-74　[Monitor] > [Monitoring Tools] > [Alarms and Events] > [Alarms] タブのフィールド（続き）

フィールド	説明
Status	アラームのステータス。
Failure Source	イベントのソース(名前や MAC アドレスを含む)を示します。
Timestamp	アラームが発生した日時。
Owner	このアラームを割り当てる個人の名前(入力された場合)。
Category	不正 AP、コントローラ、スイッチ、セキュリティなど、アラームに割り当てられたカテゴリ。
Condition	アラームの原因となった条件。
Alarm Browser ツールバー	
Change Status	アラーム ステータスを次のいずれかに変更します。 • [Acknowledge]:アラームを認知できます。デフォルトでは、認知済みのアラームは [Alarm Browser] ページに表示されません。認知済みのアラームは Prime Infrastructure に保存されるため、アラーム検索機能を使用して、認知済みのすべてのアラームを検索できます。 • [Unacknowledge]:すでに確認応答したアラームの確認応答を解除できます。 • [Clear]:選択したアラームをクリアします。アラームが [Alarm Browser] から削除されます。クリアされたアラームは Prime Infrastructure 内に残るため、アラーム検索機能を使用すると、クリアされたすべてのアラームを検索できます。
Assign	選択したアラームに対して、次を実行できます。 • [Assign to me]:アラームを自分に割り当てます。 • [Select Owner]:アラームを選択したユーザに割り当てます。 • [Unassign]:指定した所有者をアラームから削除します。
Annotation	選択したアラームに注釈を入力し、[Post] をクリックします。入力した注釈はアラームの詳細を表示するときに表示されます。
Delete	選択したアラームを削除します。アラームがどのデバイスでも検出されなくなったことを示します。

表 1-74　[Monitor] > [Monitoring Tools] > [Alarms and Events] > [Alarms] タブのフィールド（続き）

フィールド	説明
Email Notification	アラームのカテゴリと重大度レベルに基づいてアラームに電子メールによる通知を設定します。Prime Infrastructure は、指定したカテゴリのアラームが発生したときに電子メールによる通知を送信します。
Show	ドロップダウン リストには次のオプションがあります。 • [Quick Filter]：入力したテキストが含まれたアラームを表示するには、ボックスにテキストを入力します。 • [Advanced Filter]：このフィルタは、高度なアラーム検索機能を提供します。さまざまな条件（「含む」、「含まない」、「～で始まる」、「～で終わる」など）を使用して、特定のフィールドを検索できます。 • [All]：すべてのアラームが表示されます。 • [Manage Preset Filter]：以前保存したフィルタの表示と、以前保存したフィルタの編集および削除が可能です。 • [Assigned to Me]：自分に割り当てられたすべてのアラームが表示されます。 • [Unassigned Alarms]：割り当てられていないすべてのアラームが表示されます。 • Alarms in Last 5 Minutes • Alarms in Last 15 Minutes • Alarms in Last 30 Minutes • Alarms in the last hour • Alarms in the last 8 hours • Alarms in the last 24 hours • Alarms in last 7 days • [All wired alarms]：有線デバイスのすべてのアラームが表示されます。 • [All wireless alarms]：ワイヤレス デバイスのすべてのアラームが表示されます。

[Monitor] > [Monitoring Tools] > [Alarms and Events] > [Events]

次の表で、[Monitor] > [Monitoring Tools] > [Alarms and Events] > [Events] タブの各フィールドについて説明します。

表 1-75　[Monitor] > [Monitoring Tools] > [Alarms and Events] > [Events] タブのフィールド

フィールド	説明
Description	イベントの詳細情報を説明します。
Time	イベントが生成された日時を示します。
Severity	イベントの重大度を示します。使用可能なオプションは、[Critical]、[Major]、[Minor]、[Warning]、[Cleared]、または [Information] です。
Failure Source	イベントのソース（名前や MAC アドレスを含む）を示します。
Category	イベントのタイプ。[Rogue AP]、[Security]、[AP] など。
Mesh Links	メッシュ リンクの情報。
Clients	クライアントの情報。

表 1-75　[Monitor] > [Monitoring Tools] > [Alarms and Events] > [Events] タブのフィールド（続き）

フィールド	説明
Context Aware Notifications	コンテキスト認識型の通知を表示します。
Coverage Hole Event	
Access Point Name	アクセス ポイント名。
Failed Clients	カバレッジ ホールにより失敗したクライアントの数。
Total Clients	カバレッジ ホールによる影響を受けたクライアントの数。
Radio Type	該当するアクセス ポイントの無線タイプ（802.11b/g または 802.11a）。
Coverage Threshold	カバレッジしきい値の情報を表示します。
Rogue AP Events	
Vendor	不正アクセス ポイントのベンダー名または [Unknown]。
Classification Type	不正アクセス ポイントのタイプ（[Malicious]、[Friendly]、[Unclassified] など）を示します。
On Network	不正検出がどのように発生したかを示します。
Controllers	コントローラが不正を検出しました（[Yes] または [No]）。
Switch Port Trace	スイッチ ポート トレースによって不正が検出されました。[Traced but not found]、[Traced and found]、[Not traced] のいずれかで示されます。
Radio Type	この不正アクセス ポイントに該当するすべての無線タイプをリストします。
State	アラームの状態を示します。アドホック不正の可能な状態には、[Threat]、[Alert]、[Internal]、[External]、[Contained]、[Contained Pending]、および [Removed] があります。
SSID	不正アクセス ポイント無線によってブロードキャストされているサービス セット ID（SSID）。SSID がブロードキャストされない場合は空欄になります。
Adhoc Rogue Events	
Vendor	不正アクセス ポイントのベンダー名または [Unknown]。
On Network	不正検出がどのように発生したかを示します。
Controllers	コントローラが不正を検出しました（[Yes] または [No]）。
[Switch Port Trace]	スイッチ ポート トレースによって不正が検出されました。[Traced but not found]、[Traced and found]、[Not traced] のいずれかで示されます。
Radio Type	この不正アクセス ポイントに該当するすべての無線タイプをリストします。
State	アラームの状態を示します。アドホック不正の可能な状態には、[Threat]、[Alert]、[Internal]、[External]、[Contained]、[Contained Pending]、および [Removed] があります。
SSID	不正アクセス ポイント無線によってブロードキャストされているサービス セット ID（SSID）。SSID がブロードキャストされない場合は空欄になります。
Interference	
Detected By	干渉を検出したデバイスの IP アドレス。
ID	干渉を検出したデバイスの ID。
Pre Coverage Hole	
Client MAC Address	プリカバレッジ ホールによる影響を受けたクライアントの MAC アドレス。
AP MAC Address	該当するアクセス ポイントの MAC アドレス。

表 1-75　[Monitor] > [Monitoring Tools] > [Alarms and Events] > [Events] タブのフィールド（続き）

フィールド	説明
Radio Type	該当するアクセス ポイントの無線タイプ（802.11b/g または 802.11a）。
Power Level	アクセス ポイント の送信電力レベル（1 = 国コード設定ごとに許可された最大電力、2 = 50% の電力、3 = 25% の電力、4 = 6.25 ～ 12.5% の電力、5 = 0.195 ～ 6.25% の電力）。
Client Type	クライアント タイプは、laptop(0)、pc(1)、pda(2)、dot11mobilephone(3)、dualmodephone(4)、wgb(5)、scanner(6)、tabletpc(7)、printer(8)、projector(9)、videoconfsystem(10)、camera(11)、gamingsystem(12)、dot11deskphone(13)、cashregister(14)、radiotag(15)、rfidsensor(16)、server(17) です。
WLAN Coverage Hole Status	カバレッジ ホールのステータスを表示します。

[Monitor] > [Monitoring Tools] > [Clients and Users]

次の表で、[Clients and Users] ページで使用可能な設定済みのフィルタと、それらのフィルタを [Show] ドロップダウン リストから選択した場合の結果について説明します。

表 1-76　クライアント リスト フィルタ

フィルタ	結果
All	非アクティブなクライアントを含むすべてのクライアント。 **注**　一般に、[All] フィルタはフィルタなしを意味します。すべての SSID が、PMIP、WGB、または有線ゲスト クライアントなど、すべてのコントローラに接続されたすべてのクライアントを返します。
2.4 GHz Clients	2.4 GHz 無線帯域を使用しているすべてのクライアント。
5 GHz Clients	5.0 GHz 無線帯域を使用しているすべてのクライアント。
All Lightweight Clients	Lightweight AP に接続されたすべてのクライアント。
All Autonomous Clients	Autonomous AP に接続されたすべてのクライアント。
All Wired Clients	Prime Infrastructure が管理するスイッチに直接接続されたすべてのクライアント。
Associated Clients	認証されているかどうかにかかわらず、ネットワークに接続されているすべてのクライアントが表示されます。
Clients detected by MSE	有線クライアントおよびワイヤレス クライアントを含め、MSE で検出されたすべてのクライアントが表示されます。
Clients detected in last 24 hours	過去 24 時間に検出されたすべてのクライアント。
Clients Known by ISE	ISE で認証されたすべてのクライアントが表示されます。
Clients with Problems	アソシエートされている一方で、ポリシーが完了していないクライアント。
Excluded Clients	コントローラによって除外された、すべての Lightweight ワイヤレス クライアント。
FlexConnect Locally Authenticated	FlexConnect AP に接続され、ローカルに認証されたクライアント。
New Clients detected in last 24 hours	過去 24 時間に検出された新規クライアント。

表 1-76　クライアント リスト フィルタ（続き）

フィルタ	結果
On Network Clients	認証および認可を完了しており、データを送受信できるクライアント。つまり、設定されたすべてのポリシーを完了しており、ネットワーク上にあるクライアントです。クライアントはアイデンティティ クライアントではなく、常に「On Network」と表示されます。
WGB Clients	すべての WGB クライアント。 **注**　ブリッジ機能を持つアクセス ポイントの AP モードに [Bridge] を設定すると、クライアントを WGB として識別して表示できます。WGB クライアントは、無線を有線にブリッジします。Cisco IOS アクセス ポイントはすべて、有線クライアントが接続された無線クライアントとして、WGB のロールを果たすことができます。この WGB についての情報はコントローラに伝播され、Prime Infrastructure と WLC の両方にクライアントとして表示されます。

次の表に、[Clients and Users] テーブルで使用可能な列を示します。

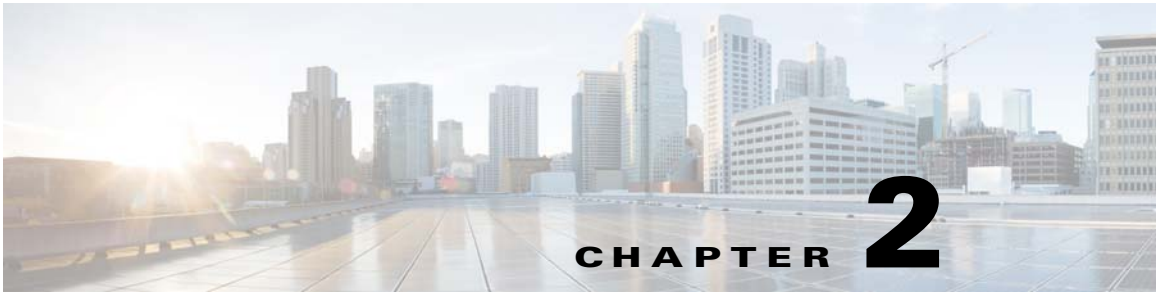
タブ	説明
Client Attributes	[Clients and Users] リストからクライアントを選択すると、そのクライアントの属性が [Clients and Users] リストに表示されます。クライアントは、MAC アドレスを使用して特定されます。 [Client Attributes] グループ ボックスに表示される詳細情報はデバイスから取得される一方で、[Clients and Users] リストに表示される詳細情報はデータベースから取得されます。したがって、[Clients and Users] リストと [Client Attributes] グループ ボックスでは、表示される詳細情報が食い違うこと場合があります。 有線クライアントの場合、この情報はスイッチから取得されます。また、詳細ページに表示されるデータは、コントローラ/スイッチ/ISE からオンデマンドで収集されたライブデータです。 これらの詳細には、次のクライアント詳細が含まれます。 • [General]:ユーザ名、MAC アドレスなどの生成情報をリストします。 ユーザ名の横にある アイコンをクリックすると、ユーザの関連するユーザにアクセスします。 • [Session]:クライアント セッション情報をリストします。 [Security](ワイヤレス クライアントおよびアイデンティティ有線クライアントのみ):セキュリティ ポリシー、認証情報、および EAP タイプをリストします。 アイデンティティ クライアントは、認証タイプが 802.1x、MAC 認証バイパス、または Web 認証のクライアントです。アイデンティティ クライアント以外の認証タイプは N/A です。 [Client Attributes] グループ ボックスに表示されるデータは、クライアントのタイプ、つまりアイデンティティ クライアントなのか非アイデンティティ クライアントなのかに応じて異なります。アイデンティティ クライアントの場合は、認証ステータス、監査セッション ID などのセキュリティ情報を確認できます。 • [Statistics](ワイヤレスのみ) • [Traffic]:クライアントのトラフィック情報を表示します。 ワイヤレス クライアントの場合、クライアントのトラフィック情報はコントローラから取得します。有線クライアントの場合、クライアントのトラフィック情報は ISE から取得するため、スイッチ上でアカウンティング情報およびその他の必要な機能を有効にする必要があります。 クライアントの統計情報を参照するには、[Refresh from Device] をクリックします。
Client Attributes Summary	クライアント、アクセス ポイント、スイッチ トポロジに対応するデバイスの 360°ビューを表示するには、そのアイコンをクリックします。

タブ	説明
Client IPv6 Addresses	[Clients and Users] リストから IPv6 クライアントを選択すると、クライアント IPv6 アドレスの詳細が表示されます。この詳細情報は、コントローラから直接取得されています。 IPv6 アドレスを持つ有線クライアントの場合は、Prime Infrastructure がスイッチの IPv6 ネイバー テーブルからクライアントのアドレスを検出します。 この詳細には、次の情報が含まれます。 • IP アドレス:クライアントの IPv6 アドレス。 • スコープ • アドレス タイプ • 検出時間
Client Statistics	クライアント統計情報には、選択したクライアントの次の情報が含まれます。 • クライアント AP アソシエーション履歴 • クライアント RSSI 履歴(dBm):クライアントがアソシエートされたアクセス ポイントで検出された RSSI(受信信号強度インジケータ)の履歴。 • クライアント SNR 履歴:クライアントがアソシエートされたアクセス ポイントで検出された SNR(クライアント RF セッションの信号対雑音比)の履歴。 RSSI および SNR の重大度レベルは、[Normal]、[Major]、[Minor]、または [Critical] として示されます。 • 送受信バイト(Kbps):アソシエートされたアクセス ポイントで送受信したバイト数。 • 送受信パケット(毎秒):アソシエートされたアクセス ポイントで送受信したパケット数。 • 経時データ レート グラフ上にマウス カーソルを合わせると、その他の統計情報が表示されます。 この情報は、インタラクティブ グラフで表示されます。詳細については、「関連項目」の「*Interactive Graphs*」の項を参照してください。

タブ	説明
Client Association History	[Association History] ダッシュレットには、選択したクライアントの過去 10 件のアソシエーション時間に関する情報が表示されます。この情報は、クライアントのトラブルシューティングに役立つことがあります。このセクションは、クライアントが正常に認証されなかった場合は空欄のままになります。 選択した期間（例えば、[6h]、[1d]、[1w] など）、次の理由により、[Client Association History] チャートが正しく表示されない場合があります。 – ローミング中にクライアントが関連付けられたアクセス ポイント（Y 軸にプロット）の数が 5 を超えている。 – 関連付けポイントと関連付け解除ポイント（X 軸にプロット）の数が 120 を超えている。 • クライアント アソシエーション履歴（ワイヤレス クライアントの場合）には、次の情報が含まれます。 – アソシエーションの日付と時刻 – アソシエーションの期間 – ユーザ名 – IP アドレス – アクセス ポイント名（ワイヤレス クライアントの場合のみ） – アクセス ポイントとコントローラ名（有線クライアントの場合のみ） – マップの場所（有線クライアントの場合のみ） – コントローラ名（ワイヤレス クライアントの場合のみ） – SSID – プロトコル – トラフィックの量（MB） – ホスト名 – ローミング理由（*コントローラから認識されなくなった、新規アソシエーションを検出したなど*） [Current Associated Clients] テーブルの列を追加、削除、並べ替えるには、設定アイコンをクリックします。設定アイコンを使用して追加できる新しいパラメータの追加については、「関連項目」の「*Configuring the List of Access Points Display*」を参照してください。 Prime Infrastructure は、アクセス ポイントの再関連付けを別のセッションとしてレポートします。この理由は次のとおりです。 • WLAN でのセッション タイムアウト • 設定中のインターフェイスによる低電力レベル • クライアントがローミング中 • クライアント ドライバの実装 クライアント ドライバでのデータ復号化エラー
Client Event Information	[Client Details] ページの [Client Event] ダッシュレットには、イベント タイプやイベントの日時など、このクライアントのすべてのイベントが表示されます。 イベント タイプの詳細を表示するには、イベント タイプをクリックします。詳細については、「関連項目」の「*Monitoring Failure Objects*」の項を参照してください。

タブ	説明
Client Location Information	選択したクライアントの次のロケーション パラメータが表示されます(該当する場合)。 • [Map Area]:クライアントが最後に検出されたマップ領域。 • [ELIN]:緊急ロケーション識別番号。MSE によって検出される有線クライアントのみに適用されます。 • [Civic Address]:[Civic Address] タブにあるフィールドは、クライアントの Civic アドレスがインポートされている場合のみ入力されます。MSE によって検出される有線クライアントのみに適用されます。 • [Advanced]:クライアントの詳細情報。このタブにあるフィールドは、クライアントの Civic アドレスがインポートされている場合のみ入力されます。 クライアントの Civic 情報のインポートの詳細については、「関連項目」の「*Configuring a Switch Location*」の項を参照してください。
Wired Location History	有線クライアントのロケーション履歴を表示できます。 有線クライアントは MSE によって検出されている必要があり、有線クライアントの履歴が MSE で有効化されている必要があります。 クライアントに関する次のロケーション履歴情報が表示されます。 • タイムスタンプ • 状態 • ポート タイプ • スロット • モジュール • ポート • ユーザ名 • IP アドレス • スイッチ IP • サーバ名 • マップ位置 • 都市ロケーション
Wireless Location History	ワイヤレス クライアントのロケーション履歴を表示できます。 ワイヤレス クライアントは MSE によって検出されている必要があり、有線クライアントの履歴が MSE で有効化されている必要があります。

タブ	説明
Client CCXv5 Information	CCXv5 クライアントは、シスコ互換の Extensions Version 5（CCXv5）をサポートするクライアント デバイスです。CCXv5 クライアントに固有のレポートにより、クライアントの診断およびトラブルシューティングを強化するクライアントの詳細が提供されます。 CCXv5 製造元情報は、CCXv5 クライアントの場合のみ表示されます。 • [Organizationally Unique Identifier]：IEEE によって割り当てられた組織固有識別子。無線ネットワーク接続デバイスの MAC アドレスの最初の 3 バイトなど。 • [ID]：無線ネットワーク アダプタの製造業者 ID。 • [Model]：無線ネットワーク アダプタのモデル。 • [Serial Number]：無線ネットワーク アダプタのシリアル番号。 • [Radio]：クライアントの無線の種類。 • [MAC Address]：クライアントに割り当てられた MAC アドレス。 • [Antenna Type]：無線ネットワーク アダプタに接続されるアンテナの種類。 • [Antenna Gain]：無線ネットワーク アダプタに接続される指向性アンテナのピーク ゲイン（dBi）、および全方向性アンテナの平均ゲイン（dBi）。ゲインは 0.5dBi の倍数で表します。整数値 4 は、4 X 0.5 = 2dBi のゲインであることを意味します。 • [Automated Troubleshooting Report]：自動テストが実行された場合、このレポートには、自動トラブルシューティングのログである AUTO_TS_LOG<ClientMac>.txt の場所が表示されます。自動化されたテストが実行されていない場合は、[Not Exists] が表示されます。n. • 電力（dBm）
Client CCXv5 Information	[Radio Receiver Sensitivity]：次の情報を含む、ワイヤレス ネットワーク アダプタの受信装置の感度が表示されます。 • Radio • データ レート • 最小および最大 RSSI [CCXV5 Capability Information]：CCXv5 クライアントに限り、Capability Information パラメータが表示されます。 • Radio • [Client Status]：成功または失敗。 • [Service Capability]：音声、ストリーミング（一方向）ビデオ、インタラクティブ（双方向）ビデオなどのサービス機能。 [Radio Channels]：該当する各無線のチャネルを識別します。 [Transmit Data Rates]：各無線の伝送データ レート（Mbps）を識別します。 [Transmit Power Values]：次の情報を含む送信電力を示します。 • 電源モード • Radio



[Configuration] ページのフィールド リファレンス

この章では、Cisco Prime Infrastructure リリース 3.0 の [Configuration] タブにあるページの各フィールドについて説明します。この章は、次の内容で構成されています。

[Network Devices] のフィールドの説明

次に、[Configuration] > [Network Devices] ページの各フィールドについて説明します。

[Wireless Controllers] > [System] > [AP 802.1X Supplicant Credentials]

表 2-10 で、[Configuration] > [Controllers] > [Network Devices] > [Controllers] > [AP 802.1X Supplicant Credentials] ページの各フィールドについて説明します。

表 2-1　[Wireless Controllers] > [System] > [AP 802.1X Supplicant Credentials]

フィールド	説明
Template Basic	
Name	テンプレートの名前を入力します。
Description	(オプション)テンプレートの説明を入力します。
Tags	タグを 1 つ以上入力します。テンプレートのグループ化にはタグを使用します。テンプレートにタグを使用する方法は、次の 2 通りあります。 • テンプレートの作成時にタグを作成する。 • または、[Template] 検索バーの下にある [Tag] アイコンを使用する。

表 2-1　[Wireless Controllers] > [System] > [AP 802.1X Supplicant Credentials]（続き）

フィールド	説明
Validation Criteria	
Device Type	ドロップダウン リストから、デバイス タイプを選択します。
Template Detail	
Global Supplicant Credential	グローバル サプリカント クレデンシャルを有効にするには、このオプションを選択します。

[Wireless Controllers] > [System] > [AP Timers]

表 2-2 で、[Configuration] > [Network Devices] > [Controllers] > [AP Timers] ページの各フィールドについて説明します。

表 2-2　[Wireless Controllers] > [System] > [AP Timers]

フィールド	説明
Access Point Mode	[Access Point Mode] は自動的に入力されます。[Access Point Mode] 列の各値は、リンクです。リンクをクリックすると、[Controller Template access point mode] ページが表示されます。 • [FlexConnect Mode]：FlexConnect モード テンプレートを設定するには、このリンクをクリックします。 • [Local Mode]：ローカル モード テンプレートを設定するには、このリンクをクリックします。
Applied to Controllers	WLAN テンプレートが適用されるコントローラの数が表示されます。
Applied to Virtual Domains	コントローラ テンプレートが適用される仮想ドメインの数が表示されます。
Last Saved At	テンプレートが最後に保存された日時を表示します。

[Wireless Controllers] > [System] > [AP Timers] > [FlexConnect Mode] > [Edit]

表 2-3 では、[Configuration] > [Network Devices] > [Controllers] > [AP Timers] > [FlexConnect Mode] > [Edit] ページの各フィールドについて説明します。

表 2-3　[Configuration] > [Network Devices] > [Controllers] > [AP Timers] > [FlexConnect Mode] > [Edit]

フィールド	説明
Template Basic	
Name	テンプレートの名前を入力します。
Description	(オプション)テンプレートの説明を入力します。
Tags	タグを 1 つ以上入力します。テンプレートのグループ化にはタグを使用します。テンプレートにタグを使用する方法は、次の 2 通りあります。 • テンプレートの作成時にタグを作成する。 • または、[Template] 検索バーの下にある [Tag] アイコンを使用する。

表 2-3　[Configuration] > [Network Devices] > [Controllers] > [AP Timers] > [FlexConnect Mode] > [Edit]（続き）

フィールド	説明
Validation Criteria	
Device Type	ドロップダウン リストから、デバイス タイプを選択します。
Template Detail	
Access Point Mode	[Access Point Mode] は自動的に入力されます。
AP Fast Heartbeat Timer State	AP 高速ハートビートのタイムアウトを有効にするには、このチェックボックスをオンにします。
	[AP Fast Heartbeat Timeout] に値を入力します。有効な範囲は 1 ～ 15 秒です。デフォルトは 10 秒です。推奨されるタイムアウト値を次に示します。 • 7500 シリーズ コントローラ:10 ～ 15 秒 • リリース 7.0.98.0 以前の 5500 シリーズ コントローラ:10 ～ 15 秒 • リリース 7.0.98.0 以降の 5500 シリーズ コントローラ:1 ～ 10 秒 その他のコントローラ:1 ～ 10 秒

[Wireless Controllers] > [System] > [AP Timers] > [Local Mode] > [Edit]

表 2-4 で、[Configuration] > [Network Devices] > [Controllers] > [AP Timers] > [Local Mode] > [Edit] ページの各フィールドについて説明します。

表 2-4　[Configuration] > [Network Devices] > [Controllers] > [AP Timers] > [Local Mode] > [Edit]

フィールド	説明
Template Basic	
Name	テンプレートの名前を入力します。
Description	(オプション)テンプレートの説明を入力します。
Tags	タグを 1 つ以上入力します。テンプレートのグループ化にはタグを使用します。テンプレートにタグを使用する方法は、次の 2 通りあります。 • テンプレートの作成時にタグを作成する。 • または、[Template] 検索バーの下にある [Tag] アイコンを使用する。
Validation Criteria	
Device Type	ドロップダウン リストから、デバイス タイプを選択します。
Template Detail	
Access Point Mode	[Access Point Mode] は自動的に入力されます。

表 2-4　[Configuration] > [Network Devices] > [Controllers] > [AP Timers] > [Local Mode] > [Edit]（続き）

フィールド	説明
AP Fast Heartbeat Timer State	AP 高速ハートビートのタイムアウトを有効にするには、このチェックボックスをオンにします。
AP Fast Heartbeat Timeout	[AP Fast Heartbeat Timeout] に値を入力します。有効な範囲は 1 ～ 15 秒です。デフォルトは 10 秒です。推奨されるタイムアウト値を次に示します。 • 7500 シリーズ コントローラ:10 ～ 15 秒 • リリース 7.0.98.0 以前の 5500 シリーズ コントローラ:10 ～ 15 秒 • リリース 7.0.98.0 以降の 5500 シリーズ コントローラ:1 ～ 10 秒 その他のコントローラ:1 ～ 10 秒

[Wireless Controllers] > [System] > [AP Username Password]

表 2-5 で、[Configuration] > [Network Devices] > [Controllers] > [AP Username Password] ページの各フィールドについて説明します。

表 2-5　[Configuration] > [Network Devices] > [Controllers] > [AP Username Password]

フィールド	説明
Template Basic	
Name	テンプレートの名前を入力します。
Description	(オプション)テンプレートの説明を入力します。
Tags	タグを 1 つ以上入力します。テンプレートのグループ化にはタグを使用します。テンプレートにタグを使用する方法は、次の 2 通りあります。 • テンプレートの作成時にタグを作成する。 • または、[Template] 検索バーの下にある [Tag] アイコンを使用する。
Validation Criteria	
Device Type	ドロップダウン リストから、デバイス タイプを選択します。
Template Detail	
AP Password	コントローラに接続するすべてのアクセス ポイントが継承するパスワードを入力します。
Confirm Password	アクセス ポイントのパスワードを再入力します。
Enable Password	Cisco IOS AP の場合は、有効化パスワードが必要です。
Confirm Enable Password	Cisco IOS アクセス ポイントの場合は、有効化パスワードも入力して確認する必要があります。

[Wireless Controllers] > [System] > [DHCP]

表 2-6 で、[Configuration] > [Network Devices] > [Controllers] > [DHCP] ページの各フィールドについて説明します。

表 2-6　[Configuration] > [Network Devices] > [Controllers] > [DHCP]

フィールド	説明
Template Basic	
Name	テンプレートの名前を入力します。
Description	(オプション)テンプレートの説明を入力します。
Tags	タグを 1 つ以上入力します。テンプレートのグループ化にはタグを使用します。テンプレートにタグを使用する方法は、次の 2 通りあります。 • テンプレートの作成時にタグを作成する。 • または、[Template] 検索バーの下にある [Tag] アイコンを使用する。
Validation Criteria	
Device Type	ドロップダウン リストから、デバイス タイプを選択します。
Template Detail	
DHCP Option 82 Remote Id field format	ドロップダウン リストから [AP-MAC]、[AP-MAC-SSID]、[AP-ETHMAC]、または [AP-NAME-SSID] を選択します。
DHCP Proxy	DHCP プロキシを有効にするには、このチェックボックスをオンにします。DHCP プロキシがコントローラ上で有効になっている場合は、コントローラによってクライアントから設定済みサーバへ DHCP 要求がユニキャストされます。少なくとも 1 つの DHCP サーバが、WLAN にアソシエートされたインターフェイスか WLAN 自体で設定されている必要があります。DHCP プロキシは、デフォルトで有効になっています。
DHCP タイムアウト	[DHCP Timeout] を秒単位で入力します。この時間を過ぎると DHCP 要求がタイムアウトされます。デフォルト設定は 5 です。有効値の範囲は 5 ～ 120 秒です。 DHCP タイムアウトは、リリース 7.0.114.74 以降のコントローラで適用されます。

[Wireless Controllers] > [System] > [Dynamic Interface]

表 2-7 で、[Configuration] > [Network Devices] > [Controllers] > [Dynamic Interface] ページの各フィールドについて説明します。

表 2-7　[Configuration] > [Network Devices] > [Controllers] > [Dynamic Interface]

フィールド	説明
Template Basic	
Name	テンプレートの名前を入力します。
Description	(オプション)テンプレートの説明を入力します。
Tags	タグを 1 つ以上入力します。テンプレートのグループ化にはタグを使用します。テンプレートにタグを使用する方法は、次の 2 通りあります。 • テンプレートの作成時にタグを作成する。 • または、[Template] 検索バーの下にある [Tag] アイコンを使用する。

表 2-7　[Configuration] > [Network Devices] > [Controllers] > [Dynamic Interface]（続き）

フィールド	説明
Validation Criteria	
Device Type	ドロップダウン リストから、デバイス タイプを選択します。
Template Detail	
Interface Address	
Guest LAN	インターフェイスを有線としてマークするには、このチェックボックスをオンにします。
Quarantine	VLAN を検疫するには、このチェックボックスをオンにします。
Netmask	インターフェイスのネット マスク アドレスを入力します。
Physical Information	
LAG Mode	リンク アグリゲーション（LAG）を有効にするには、このチェックボックスをオンにします。
Primary Port Number	プライマリ ポート番号を入力します。 プライマリおよびセカンダリのポート番号は、Cisco 4400 シリーズのワイヤレス コントローラにのみ存在します。
Secondary Port Number	セカンダリ ポートを入力します。セカンダリ ポートは、プライマリ ポートがダウンしているときにインターフェイスにより使用されます。プライマリ ポートが再アクティブ化されると、Cisco 4400 シリーズ Wireless ワイヤレス LAN コントローラは、インターフェイスをプライマリ ポートに戻します。
AP Management	アクセス ポイントの管理を有効にするには、このチェックボックスをオンにします。
DHCP Information	
Primary DHCP Server	プライマリ DHCP サーバの IP アドレスを入力します。
WINS Server	セカンダリ DHCP サーバの IP アドレスを入力します。
DHCP Proxy Mode	ドロップダウン リストから DHCP プロキシ モードのタイプを選択します。使用可能な値は [Global]、[Enabled]、および [Disabled] です。
Enable DHCP Option 82	DHCP リレー エージェント情報オプションを有効にするには、このチェック ボックスをオンにします。
Enable DHCP Option 82- Link Select	[DHCP Option 82 - Link Select] を有効にするには、このチェックボックスをオンにします。
Link Select relay source	[Select replay source] ドロップダウン リストから値を選択します。
Enable DHCP Option 82-VPN Select	[DHCP Option 82 - VPN Select] を有効にするには、このチェックボックスをオンにします。
VPN Select-VRF Name	
VPN Select-VPN ID	
Access Control List	
ACL Name	[ACL Name] ドロップダウン リストの定義済みの名前のリストから名前を選択します。
mDNS Profile	[mDNS Profile] ドロップダウン リストから、[mDNS] プロファイルを選択します。デフォルトのオプションは [none] です。

[Wireless Controllers] > [System] > [Dynamic Interface]

表 2-8 で、[Configuration] > [Network Devices] > [Controllers] > [Dynamic Interface] ページの各フィールドについて説明します。

表 2-8　[Configuration] > [Network Devices] > [Controllers] > [Dynamic Interface]

フィールド	説明
Template Basic	
Name	テンプレートの名前を入力します。
Description	(オプション)テンプレートの説明を入力します。
Tags	タグを 1 つ以上入力します。テンプレートのグループ化にはタグを使用します。テンプレートにタグを使用する方法は、次の 2 通りあります。 • テンプレートの作成時にタグを作成する。 • または、[Template] 検索バーの下にある [Tag] アイコンを使用する。
Validation Criteria	
Device Type	ドロップダウン リストから、デバイス タイプを選択します。
Template Detail	
Interface Address	
Guest LAN	インターフェイスを有線としてマークするには、このチェックボックスをオンにします。
Quarantine	VLAN を検疫するには、このチェックボックスをオンにします。
Netmask	インターフェイスのネット マスク アドレスを入力します。
Physical Information	
LAG Mode	リンク アグリゲーション(LAG)を有効にするには、このチェックボックスをオンにします。
Primary Port Number	プライマリ ポート番号を入力します。 プライマリおよびセカンダリのポート番号は、Cisco 4400 シリーズのワイヤレス コントローラにのみ存在します。
Secondary Port Number	セカンダリ ポートを入力します。セカンダリ ポートは、プライマリ ポートがダウンしているときにインターフェイスにより使用されます。プライマリ ポートが再アクティブ化されると、Cisco 4400 シリーズ Wireless ワイヤレス LAN コントローラは、インターフェイスをプライマリ ポートに戻します。
AP Management	アクセス ポイントの管理を有効にするには、このチェックボックスをオンにします。
DHCP Information	
Primary DHCP Server	プライマリ DHCP サーバの IP アドレスを入力します。
WINS Server	セカンダリ DHCP サーバの IP アドレスを入力します。
DHCP Proxy Mode	ドロップダウン リストから DHCP プロキシ モードのタイプを選択します。使用可能な値は [Global]、[Enabled]、および [Disabled] です。
Enable DHCP Option 82	DHCP リレー エージェント情報オプションを有効にするには、このチェック ボックスをオンにします。
Enable DHCP Option 82- Link Select	[DHCP Option 82 - Link Select] を有効にするには、このチェックボックスをオンにします。

表 2-8　[Configuration] > [Network Devices] > [Controllers] > [Dynamic Interface]（続き）

フィールド	説明
Link Select relay source	[Select replay source] ドロップダウン リストから値を選択します。
Enable DHCP Option 82-VPN Select	[DHCP Option 82 - VPN Select] を有効にするには、このチェックボックスをオンにします。
VPN Select-VRF Name	
VPN Select-VPN ID	
Access Control List	
ACL Name	[ACL Name] ドロップダウン リストの定義済みの名前のリストから名前を選択します。
mDNS Profile	[mDNS Profile] ドロップダウン リストから、[mDNS] プロファイルを選択します。デフォルトのオプションは [none] です。

[Wireless Controllers] > [System] > [General] > [System Field Descriptions]

表 2-10 で、[Configuration] > [Network Devices] > [Wireless Controllers] > [System] > [General] > [System] ページの各フィールドについて説明します。

表 2-9　[Wireless Controllers] > [System] > [General] > [System Field Descriptions]

フィールド	説明
802.3x Flow Control Mode	有効または無効。
802.3 Bridging	有効または無効。
Web Radius Authentication	[PAP]、[CHAP]、または [MD5-CHAP] を選択します。 • [PAP]：パスワード認証プロトコル。クリア テキストでユーザ情報（ユーザ名およびパスワード）が送信される認証方法。 • [CHAP]：チャレンジ ハンドシェイク認証プロトコル。ユーザ情報を送信用に暗号化する認証方式。 • [MD5-CHAP]：Message Digest 5 チャレンジ ハンドシェイク認証プロトコル。MD5 では、パスワードは Message Digest 5 アルゴリズムを使用してハッシュされます。
AP Primary Discovery Timeout	30 ～ 3600 秒の値を入力します。 アクセス ポイントはバックアップ コントローラのリストを維持し、リスト上の各エントリに対して定期的にプライマリ ディスカバリ要求を送信します。設定されている場合、プライマリ ディスカバリ要求タイマーは、アクセス ポイントからのプライマリ ディスカバリ要求に対して応答する時間を指定します。この時間を超えても応答がない場合は、アクセス ポイントはそのコントローラは接続できないと見なし、次にリストされているコントローラからのディスカバリ応答を待ちます。
CAPWAP Transport Mode	レイヤ 3 またはレイヤ 2。詳細については、「Lightweight Access Point Protocol Transport Mode」を参照してください。

表 2-9　[Wireless Controllers] > [System] > [General] > [System Field Descriptions]（続き）

フィールド	説明
Current LWAPP Operating Mode	自動的に読み込まれます。
Broadcast Forwarding	有効または無効。
LAG Mode	LAG を無効にするには、[Disabled] を選択します。 リンク集約（LAG）は、802.3ad ポート集約標準の部分的な実装です。コントローラのすべてのディストリビューション システム ポートが 1 つの 802.3ad ポート チャネルにまとめられるので、コントローラのポートの設定に必要な IP アドレスの数を減らすことができます。LAG が有効である場合、ポートの冗長性は動的に管理され、アクセス ポイントはユーザからは透過的にロード バランシングされます。 Cisco 5500 および 4400 シリーズ コントローラでは LAG はデフォルトで無効化されていますが、Cisco WiSM コントローラおよび Catalyst 3750G 統合型無線 LAN コントローラ スイッチのコントローラではデフォルトで有効化されます。
Ethernet Multicast Support	• [Disable]：コントローラでのマルチキャスト サポートを無効にする場合に選択します。 • [Unicast]：マルチキャスト パケットを受信した場合に、コントローラがパケットをアソシエートされたアクセス ポイントすべてに転送する場合に選択します。FlexConnect は、ユニキャスト モードのみをサポートしています。 • [Multicast]：コントローラでのマルチキャスト サポートを有効にする場合に選択します。
Aggressive Load Balancing	有効または無効。ロード バランシングの詳細については「Aggressive Load Balancing」を参照してください。
Peer to Peer Blocking Mode	• [Disable]：同じサブネットのクライアントはこのコントローラを使用して通信します。 • [Enable]：同じサブネットのクライアントは上位レベルのルータを使用して通信します。
Over Air Provision AP Mode	有効または無効。 無線プロビジョニング（OTAP）は、Cisco 5500 および 4400 シリーズ コントローラでサポートされています。この機能がコントローラ上で有効にされると、アソシエートされたアクセス ポイントすべてはワイヤレス CAPWAP または LWAPP ネイバー メッセージを送信し、新しいアクセス ポイントはこれらのメッセージからコントローラの IP アドレスを受信します。この機能はデフォルトでは無効です。すべてのアクセス ポイントをインストールする際は、無効のままにしておいてください。 コントローラ上で OTAP を無効にしても、アクセス ポイント上では OTAP は無効になりません。OTAP はアクセス ポイント上で無効化できません。
AP Fallback	有効または無効。 AP フォールバックを有効にすると、プライマリ コントローラの接続が切断されたアクセス ポイントがプライマリ コントローラの復帰と同時に自動的にサービスに戻ります。
AP Failover Priority	有効または無効。 アクセス ポイントのフェールオーバー優先度設定を設定するには、まず AP Failover Priority 機能を有効にする必要があります。詳細については、「AP Failover Priority」を参照してください。
Apple Talk Bridging	有効または無効。

表 2-9　[Wireless Controllers] > [System] > [General] > [System Field Descriptions]（続き）

フィールド	説明
Fast SSID change	有効または無効。 コントローラ上で Fast SSID Change が有効になっているときは、クライアントは SSID 間で移動することができます。クライアントが異なる SSID の新しいアソシエーションを送信すると、コントローラの通信テーブルのクライアント エントリがクリアされてから、新しい SSID にクライアントが追加されます。Fast SSID Change が無効のときは、コントローラは一定の遅延時間が経過した後でクライアントに新しい SSID への移動を許可します。 有効にすると、クライアントは SSID 間で接続をほとんど中断せずにコントローラに瞬時に接続します。
Master Controller Mode	有効または無効。 マスター コントローラは、通常、展開されたネットワークで使用されないため、マスター コントローラの設定は、リブートまたは OS コードのアップグレード時に自動的に無効になります。
Wireless Management	有効または無効。
ACL Counters	有効または無効。ヒット数は、[ACL Rule] ページに表示されます。
Multicast Mobility Mode	有効または無効。
Default Mobility Domain Name	ドメイン名を入力します。
Mobility Anchor Group Keep Alive Interval	クライアントが別のアクセス ポイントへの接続を試みるまでに許可される遅延時間を入力します。詳細については「Mobility Anchor Group Keep Alive Interval」を参照してください。 **ヒント**　マウス カーソルをパラメータのテキスト ボックスの上に移動すると、そのフィールドの有効な範囲が表示されます。
Mobility Anchor Group Keep Alive Retries	許容される再試行の回数を入力します。 **ヒント**　マウス カーソルをパラメータのテキスト ボックスの上に移動すると、そのフィールドの有効な範囲が表示されます。
RF Network Name	ネットワーク名を入力します。
User Idle Timeout (seconds)	秒単位でタイムアウトを入力します。
ARP Timeout (seconds)	秒単位でタイムアウトを入力します。

[Features and Technologies] フィールドの説明

次に、[Features and Technologies] テンプレートの各フィールドについて説明します。

[Application Visibility] フィールドの説明

アプリケーションの可視性(AV)機能では、インターネットへ送信されるトラフィックをモニタできます。トラフィック フローをモニタし、そのトラフィック フローに基づいたレポートを生成します。

表 2-10 に、[Configuration] > [Templates] > [Features and Technologies] > [Application Visibility & Control] > [Application Visibility] の各フィールドについて説明します。

表 2-10　Application Visibility

フィールド	説明
Template Detail	
Apply to Interface Role	ドロップダウン リストからインターフェイス ロールを選択します。インターフェイス ロールの作成の詳細については、『*Cisco Prime Network Control System WAN 1.1 ユーザ ガイド*』の「Controlling User Access(ユーザ アクセスの制御)」を参照してください。
Traffic Statistics	
On/Off	データ パケットに関する統計情報を収集しない場合は [Off] をクリックします。 次のことを行うことを推奨します。 • 必要最小限の一連のフィルタを設定します。 • IPv4 トラフィックのみを実行するサイトのトラフィック統計情報のみを収集します。
IPs、Subnets	IPv4 または IPv6 のトラフィック、あるいは IPv4 と IPv6 の両方のトラフィックに関するレポートを生成するオプションを選択します。
HTTP URL Visibility	
On/Off	HTTP URL の可視性に関する統計情報を収集しない場合は [Off] をクリックします。
IPs、Subnets	モニタする特定の IPv4 アドレスまたはサブネットのセットを選択し、IPv6 トラフィックに関するレポートを生成するかどうかを決定します。
Applications	モニタする特定のアプリケーション群を選択します(モニタ可能なアプリケーションは最大で 32 個です)。デフォルトでは、すべてのエンタープライズ関連の HTTP ベースのアプリケーションがリストに含まれます。
Advanced Options	ドロップダウン リストから [Sampling Rate] と [Direction] を選択します。デバイスへのパフォーマンスの影響を低減するには、モニタ対象の関連トラフィックのみを選択します。

表 2-10　Application Visibility（続き）

フィールド	説明
Application Response Time	
On/Off	アプリケーション応答時間のメトリックを収集しない場合は [Off] をクリックします。
IPs、Subnets	モニタする特定の IPv4 アドレスまたはサブネットのセットを選択し、IPv6 トラフィックに関するレポートを生成するかどうかを決定します。
Applications	モニタする特定のアプリケーション群を選択します（モニタ可能なアプリケーションは最大で 32 個です）。デフォルトでは、すべてのエンタープライズ関連の HTTP ベースのアプリケーションがリストに含まれます。
Voice/Video Metrics	
On/Off	音声/ビデオのトラフィックに関するメトリックを収集しない場合は [Off] をクリックします。
IPs、Subnets	モニタする特定の IPv4 アドレスまたはサブネットのセットを選択し、IPv6 トラフィックに関するレポートを生成するかどうかを決定します。
Applications	モニタする特定のアプリケーション群を選択します（モニタ可能なアプリケーションは最大で 32 個です）。デフォルトでは、エンタープライズ関連 RTP のエンタープライズ関連アプリケーションがすべてモニタされます。

[Controller Templates] フィールドの説明

多数のコントローラにわたって設定を変更するには、時間と手間がかかることがあります。テンプレートで必要な設定を適用し、コントローラ間で一貫性を保つことにより、時間を節約できます。新しいサービスやサイトを実装する場合は、これらのコントローラ テンプレートを使用してコントローラのパラメータや設定を定義します。そうしたパラメータや設定は後に、指定した数のワイヤレス LAN コントローラに展開できます。

次に、[Configuration] > [Templates] > [Features and Technologies] > [Controller] にあるページの各フィールドについて説明します。

- [Controller] > [802.11]
- [Controller] > [80211a or n or ac]
- [Controller] > [80211b or g or n]
- [Controller] > [CLI] > [General]
- [Controller] > [FlexConnect] > [FlexConnect AP Groups]
- [Controller] > [IPv6]
- [Controller] > [Location]
- [Controller] > [Management]
- [Controller] > [Mesh] > [Mesh Settings]
- [Controller] > [PMIP]
- [Controller] > [Security]
- [Controller] > [System]
- [Controller] > [WLANs] > [WLAN Configuration]
- [Controller] > [mDNS]

[Controller] > [802.11]

次に、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [802.11] にあるページの各フィールドについて説明します。

- [Controller] > [802.11] > [Band Select]
- [Controller] > [802.11] > [Load Balancing]
- [Controller] > [802.11] > [Media Stream]
- [Controller] > [802.11] > [Preferred Call]
- [Controller] > [802.11] > [RF Profiles]

[Controller] > [802.11] > [Band Select]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [802.11] > [Band Select] にある [Template Detail] の各フィールドについて説明します。

表 2-11　[Controller] > [802.11] > [Band Select]

フィールド	説明
Probe Cycle Count	プローブ サイクル回数として 1 ～ 10 の範囲で値を入力します。サイクル回数は、新しいクライアントの抑制サイクルの回数を設定します。デフォルトのサイクル回数は 2 です。
Scan Cycle Period Threshold	スキャン サイクル期間のしきい値として 1 ～ 1000 ミリ秒の範囲で値を入力します。この設定は、クライアントからの新しいプルーブ要求が新しいスキャン サイクルから送信される間の時間閾値を決定します。デフォルトのサイクル閾値は 200 ミリ秒です。
Age Out Suppression	エージング アウト抑制として 10 ～ 200 秒の範囲で値を入力します。エージング アウト抑制は、以前に認識されていた 802.11b/g クライアントをプルーニングするための期限切れ時間を設定します。デフォルト値は 20 秒です。この時間が経過すると、クライアントは新規とみなされて、プローブ応答抑制の対象となります。
Age Out Dual Band	エージング アウトデュアル バンドとして 10 ～ 300 秒の範囲で値を入力します。エージング アウト期間は、以前に認識されていたデュアルバンド クライアントをプルーニングするための期限切れ時間を設定します。デフォルト値は 60 秒です。この時間が経過すると、クライアントは新規とみなされて、プローブ応答抑制の対象となります。
Acceptable Client RSSI	許容されるクライアント受信信号強度インジケータ（RSSI）として -20 ～ -90 dBm の範囲で値を入力します。このフィールドは、クライアントがプローブに応答するための最大 RSSI を設定します。デフォルト値は -80 dBm です。

[Controller] > [802.11] > [Load Balancing]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [802.11] > [Load Balancing] にある [Template Detail] の各フィールドについて説明します。

表 2-12　[Controller] > [802.11] > [Load Balancing]

フィールド	説明
Client Window Size	1 ～ 20 の範囲の数を入力してください。このページ サイズは、アクセス ポイントの負荷が高すぎてそれ以上はクライアント アソシエーションを受け付けることができないかどうかを判断するアルゴリズムで使用されます。 ロード バランシング ページ + 最も負荷が低い AP 上のクライアント アソシエーション数 = ロード バランシング閾値
Max Denial Count	0 ～ 10 の範囲の数を入力してください。拒否数は、ロード バランシング中のアソシエーション拒否の最大数を設定します。

[Controller] > [802.11] > [Media Stream]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [802.11] > [Media Stream] にある [Template Detail] の各フィールドについて説明します。

表 2-13　[Controller] > [802.11] > [Media Stream]

フィールド	説明
Media Stream Name	メディア ストリームの名前を入力します。
Multicast Destination Start IP	マルチキャストまでのメディア ストリームの開始 IP アドレスを入力します。
Multicast Destination End IP	マルチキャストまでのメディア ストリームの終了 IP アドレスを入力します。開始 IP および終了 IP は、コントローラ バージョン 7.2.x 以降は、IPv4 または IPv6 マルチキャスト アドレスにすることができます。
Maximum Expected Bandwidth	メディア ストリームが使用できる最大帯域幅を入力します。
Average Packet Size	メディア ストリームが使用できる平均パケット サイズを入力します。
RRC Periodical Update	定期的に更新されるリソース予約コントロール(RRC)の計算を入力します。無効にすると、RRC の計算は、クライアントがメディア ストリームに加入したときに、1 回のみ行われます。
RRC Priority	RRC の優先度を 1(最高) ～ 8(最低)までの値で入力します。
Traffic Profile Violation	ドロップダウン リストから [Traffic Profile Violation] を選択します。このドロップダウン リストは、ストリームが QoS ビデオ プロファイルに違反したときに、ストリームがドロップされたか、ベスト エフォート キューに入れられた場合に表示されます。
Policy	ドロップダウン リストから [Policy] を選択します。このドロップダウン リストは、メディア ストリームが許可または拒否された場合に表示されます。

[Controller] > [802.11] > [Preferred Call]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [802.11] > [Preferred Call] にある [Template Detail] の各フィールドについて説明します。

表 2-14　[Controller] > [802.11] > [Preferred Call]

フィールド	説明
Number Id	優先番号を識別する値を入力します。優先コール番号は最大 6 つまで入力できます。有効な範囲は 1 ～ 6 です。デフォルト値は 1 です。
Preferred Number	優先電話番号を入力します。

[Controller] > [802.11] > [RF Profiles]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [802.11] > [RF Profiles] にある [Template Detail] の各フィールドについて説明します。

表 2-15　[Controller] > [802.11] > [RF Profiles]

フィールド	説明
Template Name	テンプレートの名前を入力します。
Profile Name	現在のプロファイルの名前を入力します。
Description	テンプレートの説明を入力します。
Radio Type	ドロップダウン リストからアクセス ポイントの無線タイプを選択します。
Minimum Power Level Assignment (-10 to 30 dBm)	最小電源レベルの割り当てとして -10 ～ 30 dBm の範囲で値を入力します。デフォルト値は -10 dBm です。
Maximum Power Level Assignment (-10 to 30 dBm)	最大電源レベルの割り当てとして -10 ～ 30 dBm の範囲で値を入力します。デフォルト値は 30 dBm です。
Power Threshold v1(-80 to -50 dBm)	電源しきい値 v1 として -80 ～ -50 dBm の範囲で値を入力します。デフォルト値は -70 dBm です。

表 2-15　[Controller] > [802.11] > [RF Profiles]（続き）

フィールド	説明
Power Threshold v2 (-80 to -50 dBm)	電源しきい値 v2 として -80 ～ -50 dBm の範囲で値を入力します。デフォルト値は -67 dBm です。
Data Rates	アクセス ポイントとクライアント間でデータを送信できるレートを指定するには、ドロップダウン リストからデータ レートを選択します。次のデータ レートが使用可能です。 • [802.11a]：6、9、12、18、24、36、48、および 54 Mbps。 • [802.11b/g]：1、2、5.5、6、9、11、12、18、24、36、48、または 54 Mbps。 また、データ レートごとに、次のオプションのいずれかを選択する必要があります。 • [Mandatory]：このコントローラ上のアクセス ポイントに関連付けるには、クライアントがこのデータ レートをサポートしている必要があります。 • [Supported]：関連付けられたクライアントは、このデータ レートをサポートしていれば、このレートを使用してアクセス ポイントと通信できます。ただし、クライアントがこのレートを使用できなくても、関連付けは可能です。 • [Disabled]：通信に使用するデータ レートは、クライアントが指定します。

[Controller] > [80211a or n or ac]

次に、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [80211a or n or ac] にあるページの各フィールドについて説明します。

- [Controller] > [80211a or n or ac] > [dot11a-RRM] > [DCA]
- [Controller] > [80211a or n or ac] > [dot11a-RRM] > [Intervals]
- [Controller] > [80211a or n or ac] > [dot11a-RRM] > [TPC]
- [Controller] > [80211a or n or ac] > [dot11a-RRM] > [Thresholds]
- [Controller] > [80211a or n or ac] > [802.11h]
- [Controller] > [80211a or n or ac] > [CleanAir]
- [Controller] > [80211a or n or ac] > [EDCA Parameters]
- [Controller] > [80211a or n or ac] > [High Throughput (802.11n)]
- [Controller] > [80211a or n or ac] > [Media Parameters] > [General]
- [Controller] > [80211a or n or ac] > [Media Parameters] > [Video]
- [Controller] > [80211a or n or ac] > [Media Parameters] > [Voice]
- [Controller] > [80211a or n or ac] > [Parameters]
- [Controller] > [80211a or n or ac] > [Roaming Parameters]

[Controller] > [80211a or n or ac] > [dot11a-RRM] > [DCA]

[Radio Resource Management (RRM) Dynamic Channel Assignment (DCA)] ページを使用して、このコントローラのチャネル幅のほか、DCA チャネルを選択できます。

RRM DCA は、5 GHz 帯域で 802.11n 40 MHz チャネルをサポートします。より高い帯域幅を使用すると、瞬間的データ レートが高くなります。

注　大きい帯域幅を選択すると、オーバーラッピングしないチャネルが減少するため、展開によっては全体のネットワーク スループットが低下することがあります。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [80211a or n or ac] > [dot11a-RRM] > [DCA] にある [Template Detail] の各フィールドについて説明します。

表 2-16　[Controller] > [80211a or n or ac] > [dot11a-RRM] > [DCA]

フィールド	説明
Assignment Mode	ドロップダウン リストから、次の 3 つのモードのいずれかを選択します。 • [Automatic]：送信電力は、この操作を許可するすべてのアクセス ポイントで定期的に更新されます。 • [On Demand]：送信電力は、[Assign Now] をクリックすると更新されます。 • [Disabled]：動的な送信電力の割り当ては行われず、値はグローバル デフォルトに設定されます。
Avoid Foreign AP	[Enable] チェックボックスをオンにすると、チャネルを割り当てる際に、RRM が外部 Cisco アクセス ポイント（RF/モビリティ ドメイン外の Cisco 以外のアクセス ポイント）からの干渉を考慮します。RRM でこの干渉を無視するには、このチェックボックスをオフにします。外部アクセス ポイントからの干渉エネルギー（dB）および負荷（使用率）が著しい特定の状況では、RRM は、この外部アクセス ポイントの近くのアクセス ポイントのこれらのチャネル（および場合により隣接チャネル）を回避するために、チャネル割り当てを調整することがあります。この調整によって、キャパシティが増加し、Cisco WLAN ソリューションの変動性が減少します。
Avoid Cisco AP Load	[Enable] チェックボックスをオンにすると、アクセス ポイントにチャネルを割り当てる際に、コントローラによって各アクセス ポイントによって使用されるトラフィック帯域幅が考慮されます。RRM でこの値を無視するには、このチェックボックスをオフにします。特定の状況でより高密度に展開されている場合、完全なチャネルの再使用を適切に作成するには、チャネルが十分に存在しないことがあります。このような状況で、RRM は、より大きなトラフィック負荷を伝送するアクセス ポイントに、より良い再使用パターンを割り当てることができます。
Avoid non 802.11 Noise	[Enable] チェックボックスをオンにすると、アクセス ポイントは、アクセス ポイント以外のノイズ源（電子レンジや Bluetooth デバイスなど）からの干渉があるチャネルを回避します。RRM でこの干渉を無視するには、このチェックボックスをオフにします。非 802.11 ノイズ源からの干渉エネルギー（dB）が著しい特定の状況では、このノイズ源の近くのアクセス ポイントのこれらのチャネル（および場合により隣接チャネル）を回避するため、RRM がチャネル割り当てを調整することがあります。この調整によって、キャパシティが増加し、Cisco WLAN ソリューションの変動性が減少します。
Signal Strength Contribution	常に有効になっています（変更不可）。Signal Strength Contribution は常に RF/モビリティ ドメイン内のすべてのアクセス ポイントの相対位置をモニタし、最適に近いチャネルの再使用を保証します。その結果、Cisco WLAN Solution キャパシティについては増加、チャネル相互および隣接チャネルの干渉については減少となります。

表 2-16　[Controller] > [80211a or n or ac] > [dot11a-RRM] > [DCA]（続き）

フィールド	説明
Event Driven RRM	[Enable] チェックボックスをオンにし、スペクトル イベント駆動型 RRM を無効にします。デフォルトでは、[Event Driven RRM] は有効です。CleanAir 対応アクセス ポイントが重大なレベルの干渉を検出すると、イベント駆動型 RRM が使用されます。
Sensitivity Threshold	[Event Driven RRM] が有効の場合、このフィールドには、イベント駆動型 RRM が生成されるしきい値レベルが表示されます。値は、[Low]、[Medium]、または [High] のいずれかになります。アクセス ポイントの干渉が閾値レベルを上回ると、RRM はローカルの動的チャネル割り当て（DCA）の実行を開始し、ネットワークのパフォーマンスを改善するために可能な場合は影響を受けるアクセス ポイント無線のチャネルを変更します。[Low] は、環境の変更に対する感度を下げることを表すのに対して、[High] は、感度を上げることを表します。

[Controller] > [80211a or n or ac] > [dot11a-RRM] > [Intervals]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [80211a or n or ac] > [dot11a-RRM] > [Intervals] にある [Template Detail] の各フィールドについて説明します。

表 2-17　[Controller] > [80211a or n or ac] > [dot11a-RRM] > [Intervals]

フィールド	説明
Neighbor Packet Frequency	各アクセス ポイントに対して強度測定を行う間隔を入力します。デフォルトは 300 秒です。
Channel Scan Duration	各アクセス ポイントに対してノイズおよび干渉測定を行う間隔を入力します。デフォルトは 300 秒です。
Load Measurement Interval	各アクセス ポイントに対して負荷測定を行う間隔を入力します。デフォルトは 300 秒です。 **注**　このパラメータは Cisco WLC Release 4.3 以降には適用できません。
Coverage Measurement Interval	各アクセス ポイントに対してカバレッジ測定を行う間隔を入力します。デフォルトは 300 秒です。 **注**　このパラメータは Cisco WLC Release 4.3 以降には適用できません。

[Controller] > [80211a or n or ac] > [dot11a-RRM] > [TPC]

コントローラは、リアルタイムの無線 LAN 状況に基づいて、アクセス ポイントの送信電力を動的に制御します。通常は、送信電力を低く維持することでキャパシティを増やし、干渉を減らします。コントローラは、3 番めに送信電力の強いネイバーによるアクセス ポイントの認識に応じて、アクセス ポイントの送信電力の調整を試行します。

送信電力コントロール（TPC）アルゴリズムは、RF 環境での変更に応じてアクセス ポイントの電力の増大と低減の両方を行います。ほとんどの場合、TPC は干渉を減らすためにアクセス ポイントの電力を下げようとしますが、アクセス ポイントで障害が発生したり、アクセス ポイントが無効になるなど、RF カバレッジで急な変更が発生した場合、TPC は周辺のアクセス ポイントで電力を増大することもあります。この機能は、カバレッジ ホール検出とは異なります。カバレッジ ホールの検出は主にクライアントと関係がありますが、TPC はアクセス ポイント間におけるチャネルの干渉を最小限に抑えながら、必要なカバレッジ レベルを達成するため、十分な RF パワーを提供する必要があります。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [80211a or n or ac] > [dot11a-RRM] > [TPC] にある [Template Detail] の各フィールドについて説明します。

表 2-18　[Controller] > [80211a or n or ac] > [dot11a-RRM] > [TPC]

フィールド	説明
TPC Version	ドロップダウン リストから [TPCv1] または [TPCv2] を選択します。 **注**　[TPCv2] オプションは、バージョン 7.2.x 以降のコントローラだけで使用できます。
Dynamic Assignment	[Dynamic Assignment] ドロップダウン リストから、次の 3 つのモードのいずれかを選択します。 • [Automatic]：送信電力は、この操作を許可するすべてのアクセス ポイントで定期的に更新されます。 • [On Demand]：送信電力は、[Assign Now] をクリックすると更新されます。 • [Disabled]：動的な送信電力の割り当ては行われず、値はグローバル デフォルトに設定されます。
Maximum Power Assignment	割り当てる最大電力を指定します。範囲：-10 ～ 30 dB。デフォルト：30 dB。
Minimum Power Assignment	割り当てる最小電力を指定します。範囲：-10 ～ 30 dB。デフォルト：30 dB。
Dynamic Tx Power Control	送信電力の動的制御を有効にするには、このチェックボックスをクリックします。
Transmitted Power Threshold	送信電力のしきい値を -50 ～ -80 の範囲で入力します。
Control Interval	送信電力制御の間隔を秒単位で表示します（読み取り専用）。

[Controller] > [80211a or n or ac] > [dot11a-RRM] > [Thresholds]

このオプションを使用して、負荷、干渉、ノイズ、カバレッジなど、さまざまな RRM しきい値を設定するテンプレートを作成または変更します。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [80211a or n or ac] > [dot11a-RRM] > [Thresholds] にある [Template Detail] の各フィールドについて説明します。

注　これらの RRM しきい値の値を適用する前に、802.11a/n/ac ネットワークを無効にする必要があります。

表 2-19　[Controller] > [80211a or n or ac] > [dot11a-RRM] > [Thresholds]

フィールド	説明
Min Failed Clients	現在コントローラにアソシエートされている故障したクライアントの最小数を入力します。
Coverage Level	カバレッジしきい値の対象範囲を入力します（dB）。

表 2-19　[Controller] > [80211a or n or ac] > [dot11a-RRM] > [Thresholds]（続き）

フィールド	説明
Signal Strength	[Coverage Level] フィールドを調整すると、[Signal Strength (dBm)] の値にこの変更が自動的に反映されます。[Signal Strength] フィールドにより、カバレッジ レベルを調整するときの信号強度に関する情報が提供されます。
Data RSSI	[Data RSSI]（−60 ～ −90 dBm）を入力します。この数値は、クライアントがアクセス ポイントにアソシエートするために必要なデータの最小受信信号強度インジケータ（RSSI）の値を示します。
Voice RSSI	[Voice RSSI]（−60 ～ −90 dBM）を入力します。この数値は、クライアントがアクセス ポイントにアソシエートするために必要な音声の最小受信信号強度インジケータ（RSSI）の値を示します。
Max. Clients	コントローラに関連付けることができるクライアントの最大数を入力します。
RF Utilization	この無線タイプのしきい値の割合を入力します。
Interference Threshold	干渉しきい値を 0 ～ 1002347 の範囲で入力します。
Noise Threshold	ノイズしきい値を -127 ～ 0 dBm の範囲で入力します。このしきい値を超えると、コントローラは Prime Infrastructure にアラームを送信します。
Coverage Exception Level Per AP	カバレッジ例外レベルの割合を入力します。最小クライアント数に設定されたカバレッジから、この割合分だけ減少した場合に、カバレッジ ホールが生成されます。

[Controller] > [80211a or n or ac] > [802.11h]

802.11h では、チャネルの変更がクライアント デバイスに通知されます。また、クライアント デバイスの送信電力を制限できるようになっています。802.11h パラメータ（電力制限およびチャネル コントローラ通知）を設定するテンプレートを作成または変更し、これらの設定を複数のコントローラに適用します。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [80211a or n or ac] > [802.11h] にある [Template Detail] の各フィールドについて説明します。

表 2-20　[Controller] > [80211a or n or ac] > [802.11h]

フィールド	説明
Power Constraint	アクセス ポイントによる現在のチャネルでの転送を停止する場合、[Power Constraint] チェックボックスをオンにします。
Channel Announcement	[Channel Announcement] チェックボックスを選択してチャネル通知を有効にします。チャネル通知は、新しいチャネルや新しいチャネル番号に切り替わった場合に、アクセス ポイントが通知するメソッドです。

[Controller] > [80211a or n or ac] > [CleanAir]

このオプションを使用して、802.11a/n/ac 無線の CleanAir パラメータを設定するテンプレートを作成または変更します。テンプレートを設定して、CleanAir を有効または無効にできます。また、レポートおよびアラームに含める干渉デバイスのタイプを設定できます。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [80211a or n or ac] > [CleanAir] にある [Template Detail] の各フィールドについて説明します。

表 2-21　[Controller] > [80211a or n or ac] > [CleanAir]

フィールド	説明
Report Interferers	[Report Interferers] チェックボックスをオンにして、CleanAir システムで干渉源を検出してレポートできるようにします。コントローラが干渉源をレポートしないようにするには、これを選択解除します。デフォルト値はオフです。
Interferers Ignored/Selected for Reporting	CleanAir システムに検出およびレポートされる必要のある干渉源が [Interferences to Detect] ボックスに表示され、検出される必要のない干渉源が [Interferers to Ignore] ボックスに表示されていることを確認してください。[>] および [<] ボタンを使用して、これらの 2 つのボックス間で干渉源を移動します。デフォルトでは、すべての干渉源が無視されます。
Persistent Device Propagation	CleanAir で検出できる持続性デバイスに関する情報を伝播できるようにするには、[Persistent Device Propagation] チェックボックスを選択します。持続性デバイスの伝播によって、干渉タイプに関する情報を指定して、この情報を近隣のアクセス ポイントに伝播できます。永続型の干渉源は、検出されない場合でも、常に存在し、WLAN の動作に干渉します。
Air Quality Alarm	[Air Quality Alarm] チェックボックスをオンにして、電波品質アラームのトリガーを有効にします。この機能を無効にするには、このボックスを選択解除します。
Air Quality Alarm Threshold	[Air Quality Alarm] チェックボックスをオンにした場合は、[Air Quality Alarm Threshold] フィールドに 1 ～ 100 の範囲で値を入力して、電波品質アラームが生成されるしきい値を指定します。電波品質が閾値レベルを下回ると、アラームが生成されます。値 1 は最低の電波品質を表し、100 は最高を表します。デフォルト値は 1 です。
Air Quality Unclassified Category Alarm	未分類の干渉源カテゴリについてアラームを生成できるようにするには、[Air Quality Unclassified category Alarm] チェックボックスをオンにします。CleanAir は、未分類の干渉源を検出してモニタできます。未分類の干渉源は、検出はされるものの、既知のいずれの干渉タイプにも対応しない干渉源です。
Air Quality Unclassified Category Severity Threshold	[Air Quality Unclassified Category Alarm] チェックボックスをオンにした場合、[Air Quality Unclassified Category Severity Threshold] テキスト ボックスに 1 ～ 99 の範囲で値を入力して、未分類カテゴリのアラームを生成するしきい値を指定します。デフォルトは 20 です。
Interferers For Security Alarm	[Interferers For Security Alarm] チェックボックスをオンにして、指定したデバイス タイプによって検出されたときに干渉源アラームをトリガーするようにします。この機能を無効にするには、このボックスを選択解除します。デフォルト値はオフです。
Interferers Ignored/Selected for Security Alarms	干渉デバイス アラームを生成する必要のある干渉源が [Interferers Selected for Security Alarms] に表示され、干渉デバイス アラームを生成する必要のない干渉源が [Interferers Ignored for Security Alarms] に表示されていることを確認してください。[>] および [<] ボタンを使用して、これらの 2 つのボックス間で干渉源を移動します。デフォルトでは、セキュリティ アラームに対してすべての干渉源が無視されます。

[Controller] > [80211a or n or ac] > [EDCA Parameters]

Enhanced Distributed Channel Access（EDCA）パラメータは、音声、ビデオ、およびその他の Quality of Service（QoS）トラフィックに優先的な無線チャネル アクセスを提供するように設計されています。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [80211a or n or ac] > [EDCA Parameters] にある [Template Detail] の各フィールドについて説明します。

表 2-22　[Controller] > [80211a or n] > [EDCA Parameters]

フィールド	説明
EDCA Profile	[EDCA Profile] ドロップダウン リストで、次のいずれかのオプションを選択します。 • [WMM]：Wi-Fi Multimedia（WMM）のデフォルト パラメータを有効にします。これはデフォルト値です。音声サービスまたはビデオ サービスがネットワーク上に展開されていない場合に、このオプションを選択します。 • [Spectralink Voice Priority]：Spectralink 音声優先パラメータを有効にします。通話の質を向上するため、ネットワークに Spectralink 電話技術を実装している場合に、このオプションを選択します。 • [Voice Optimized]：音声用に最適化された EDCA プロファイル パラメータを有効にします。Spectralink 以外の音声サービスをネットワーク上で展開している場合に、このオプションを選択します。 • [Voice & Video Optimized]：音声とビデオ用に最適化された EDCA プロファイル パラメータを有効にします。ネットワーク上で音声サービスとビデオ サービスを両方とも展開する場合に、このオプションを選択します。 **注**　ビデオ サービスは、アドミッション制御（ACM）とともに展開する必要があります。ACM なしのビデオ サービスはサポートされていません。 **注**　無線インターフェイスをシャットダウンしてから、EDCA パラメータを設定してください。
Low Latency MAC	ネットワーク上のすべてのクライアントが WMM 準拠の場合にだけ、低遅延 MAC を有効にしてください。

[Controller] > [80211a or n or ac] > [High Throughput (802.11n)]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [80211a or n or ac] > [High Throughput (802.11n)] にある [Template Detail] の各フィールドについて説明します。

表 2-23　[Controller] > [80211a or n or ac] > [High Throughput (802.11n)]

フィールド	説明
802.11n Network Status Enabled	高いスループットを可能にするには、[802.11n Network Status Enabled] チェックボックスを選択します。
Selected MCS Indexes	サポートするデータ レートのレベルを選択します。変調符号化方式（MCS）は 802.11a データ レートと類似しています。デフォルトは 20 MHz で、ショート ガード インターバルです。番号付きのデータ レートの横にある [Supported] チェックボックスをオンにすると、選択した番号が列の下部にある [Selected MCS Indexes] フィールドに表示されます。

[Controller] > [80211a or n or ac] > [Media Parameters] > [General]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [80211a or n or ac] > [Media Parameters] > [General] にある [Template Detail] の各フィールドについて説明します。

表 2-24　[Controller] > [80211a or n or ac] > [Media Parameters] > [General]

フィールド	説明
Maximum Media Bandwidth (0 to 85%)	許容する最大帯域幅のパーセンテージを指定します。このオプションは、CAC が有効の場合のみ使用可能です。

[Controller] > [80211a or n or ac] > [Media Parameters] > [Video]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [80211a or n or ac] > [Media Parameters] > [Video] にある [Template Detail] の各フィールドについて説明します。

表 2-25　[Controller] > [80211a or n or ac] > [Media Parameters] > [Video]

フィールド	説明
Admission Control (ACM)	アドミッション コントロールを有効にするには、このチェック ボックスをオンにします。
Maximum Bandwidth Allowed	許容する最大帯域幅のパーセンテージを指定します。このオプションは、CAC が有効の場合のみ使用可能です。
Reserved Roaming Bandwidth	予約するローミング帯域幅のパーセンテージを指定します。このオプションは、CAC が有効の場合のみ使用可能です。
CAC Method	[Admission Control (ACM)] が有効になっている場合は、CAC 方式を負荷ベースまたはスタティックに指定します。負荷ベースの CAC で取り入れられている測定方式では、それ自体からのすべてのトラフィック タイプによって同一チャネル アクセス ポイントで消費される帯域幅や、同一チャネルの干渉によって消費される帯域幅が考慮されています。load-based の CAC では、PHY およびチャネル欠陥の結果発生する追加の帯域幅消費も対象となります。
Unicast Video Redirect	ビデオ キュー内のすべての非メディア ストリーム パケットがベスト エフォート キューにリダイレクトされるようにするには、[Unicast Video Redirect] チェックボックスをオンにします。無効にすると、ビデオ マーキングのあるパケットはすべてのビデオ キューに保持されます。
Client Minimum Phy Rate	クライアントがメディア ストリームに加入するために必要な物理データ レートを [Client Minimum Phy Rate] ドロップダウン リストから指定します。
Multicast Direct Enable	この無線上の任意の WLAN で Media Direct を有効にするには、[Multicast Direct Enable] チェックボックスを選択します。
Maximum Number of Streams per Radio	許容する無線ごとのストリームの最大数を指定します。
Maximum Number of Streams per Client	許容するクライアントごとのストリームの最大数を指定します。
Best Effort QOS Admission	新しいクライアント要求をベスト エフォート キューにリダイレクトするには、[Best Effort QOS Admission] チェックボックスをオンにします。これは、すべてのビデオ帯域幅が使用されている場合のみ発生します。これが無効になっており、最大のビデオ帯域幅が使用されている場合は、新しいクライアント要求が拒否されます。

[Controller] > [80211a or n or ac] > [Media Parameters] > [Voice]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [80211a or n or ac] > [Media Parameters] > [Voice] にある [Template Detail] の各フィールドについて説明します。

表 2-26　[Controller] > [80211a or n or ac] > [Media Parameters] > [Voice]

フィールド	説明
Admission Control (ACM)	アドミッション コントロールを有効にするには、このチェック ボックスをオンにします。VoIP 通話中にエンド ユーザが許容できる音声品質と感じるよう、パケットはエンドポイントから別のエンドポイントまで低遅延、低パケット損失で配送される必要があります。異なるネットワーク負荷の下で QoS を維持するには、コール アドミッション制御（CAC）が必要です。アクセス ポイントでの CAC により、アクセス ポイントは、ネットワークの輻輳時でも QoS が制御された状態を維持し、許容する最大の通話数を許容できる数に保つことができます。
CAC Method	[Admission Control (ACM)] が有効になっている場合は、CAC 方式を負荷ベースまたはスタティックに指定します。負荷ベースの CAC で取り入れられている測定方式では、それ自体からのすべてのトラフィック タイプによって同一チャネル アクセス ポイントで消費される帯域幅や、同一チャネルの干渉によって消費される帯域幅が考慮されています。load-based の CAC では、PHY およびチャネル欠陥の結果発生する追加の帯域幅消費も対象となります。
Maximum Bandwidth Allowed	許容する最大帯域幅のパーセンテージを指定します。このオプションは、CAC が有効の場合のみ使用可能です。
Reserved Roaming Bandwidth	予約するローミング帯域幅のパーセンテージを指定します。このオプションは、CAC が有効の場合のみ使用可能です。
Expedited Bandwidth	緊急コール用に CAC の拡張として優先帯域幅を有効にするには、このチェックボックスを選択します。より高い優先度が TSPEC 要求に与えられるように、CCXv5 準拠の優先帯域幅の IE が必要となります。
SIP CAC	SIP CAC を有効にするには、このチェックボックスをオンにします。SIP CAC は、ステータス コード 17 をサポートし、TSPEC ベースのアドミッション制御をサポートしない電話のみに使用する必要があります。
SIP Codec	この無線で使用するコーデック名を指定します。使用可能なオプションは、[G.711]、[G.729]、および [User Defined] です。
SIP Call Bandwidth	ネットワークで SIP コールごとに割り当てる帯域幅（キロビット/秒単位）を指定します。このフィールドは、選択されている [SIP Codec] が [User Defined] である場合のみ設定できます。
SIP Sample Interval	コーデックを動作させる必要があるサンプル間隔（ミリ秒）を指定します。
Metric Collection	メトリック収集を有効にするには、このチェックボックスをオンにします。トラフィック ストリーム メトリックは、ワイヤレス LAN での VoIP に関する一連の統計情報で、ワイヤレス LAN の QoS を通知します。アクセス ポイントで測定値を収集するには、トラフィック ストリーム メトリックが有効であることが必要です。これを有効にすると、コントローラは、関連付けられたすべてのアクセス ポイントから、90 秒ごとに 802.11b/g インターフェイスに関する統計情報データの収集を開始します。VoIP またはビデオを使用している場合は、この機能を有効にする必要があります。

[Controller] > [80211a or n or ac] > [Parameters]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [80211a or n or ac] > [Parameters] にある [Template Detail] の各フィールドについて説明します。

表 2-27　[Controller] > [80211a or n or ac] > [Parameters]

フィールド	説明
802.11a Network Status	802.11a/n ネットワーク ステータスを有効にするには、このチェックボックスをオンにします。
Client Link	このドロップダウン リストからは、ClientLink をサポートするすべてのアクセス ポイント 802.11a/n 無線で ClientLink を有効にします。それ以外の場合は [Disable] を選択します。
Beacon Period	ビーコンの間隔をミリ秒単位で入力します。有効な範囲は 20 ～ 1000 ミリ秒です。
DTIM Period	配送数テキスト ボックスが 0 のトラフィック インジケータ メッセージ（TIM）要素を含むビーコン フレームの送信間に経過する可能性のあるビーコン間隔を入力します。この値は、ビーコン フレームの DTIM Period フィールドで送信されます。DTIM を追加したビーコンをクライアント デバイスが受信すると、通常は、保留中のパケットをチェックするためにクライアント デバイスが再起動します。DTIM の間隔が長くなると、クライアントのスリープ時間が長くなり、電力を節約できます。反対に、DTIM の間隔が短くなるとパケットの受信の遅延を抑えられますが、クライアントが頻繁に起動するためバッテリ残量が消費されます。
Fragmentation Threshold	パケットを断片化する（1 ブロックではなく、いくつかの断片として送信する）サイズを指定します。通信状態の悪いエリアや電波干渉が非常に多いエリアでは、低い数値を設定します。
802.11e Max Bandwidth	802.11e の最大帯域幅のパーセンテージを入力します。
Mode	Cisco Compatible Extensions（CCX）位置測定を有効にするには、このチェックボックスをオンにします。有効な場合、これによってクライアントの位置の正確さが向上します。
Interval	CCX 位置測定信号をブロードキャストする間隔を秒単位で入力します。Cisco Compatible Extension の CCX 位置測定間隔を変更できるのは、測定モードが有効になっている場合だけです。
Data Rate Dropdowns	各データ レートのネゴシエーション タイプを選択します。クライアントおよびコントローラは、データ レートをネゴシエートします。データ レートが [Mandatory] に設定されている場合、クライアントはネットワークを使用するには、そのデータ レートをサポートしている必要があります。データ レートがコントローラで [Supported] として設定されている場合は、同じレートをサポートしており、関連付けられているクライアントはそのレートを使用してアクセス ポイントと通信する可能性があります。しかし、アソシエートするために、サポートされるすべてのレートをクライアントが使用する必要はありません。それぞれのレートについて、[Mandatory] または [Supported] のドロップダウン リストが使用可能です。各データ レートは、[Disabled] に設定し、クライアントの設定に合わせることもできます。
Channel List	[Noise/Interference/Rogue Monitoring Channels] セクションのこのドロップダウン リストから、必要なモニタリング レベルに基づいて、すべてのチャネル、各国のチャネル、または DCA チャネルから選択します。DCA により、コントローラに接続された管理対象デバイスの中から妥当なチャネルの割り当てが自動的に選択されます。

[Controller] > [80211a or n or ac] > [Roaming Parameters]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [80211a or n or ac] > [Roaming Parameters] にある [Template Detail] の各フィールドについて説明します。

表 2-28　[Controller] > [80211a or n or ac] > [Roaming Parameters]

フィールド	説明
Mode	[Mode] ドロップダウン リストを使用して、[Default] の値、または [Custom] の値のいずれかのコンフィギュレーション モードを選択します。[Default] を選択した場合は編集にローミング パラメータが使用できなくなり、テキスト ボックスにデフォルト値が表示されます。ローミング パラメータを編集するには、[Custom] を選択します。
Minimum RSSI	クライアントをアクセス ポイントに関連付けるときに必要な受信信号強度インジケータ（RSSI）の最小値を入力します。クライアントの平均の受信信号の強度がこの閾値より低い場合、通常、信頼できる通信はできません。したがって、最小の RSSI 値に達する前に、クライアントはより強い信号のある別のアクセス ポイントをすでに見つけてローミングしている必要があります。範囲：-80 ～ -90 dBm。デフォルト：-85 dBm。
Roaming Hysteresis	クライアントがローミングするために必要な、隣接するアクセス ポイントの信号強度の値を入力します。このフィールドは、クライアントが物理的に 2 つのアクセス ポイントの境界上やその近くにある場合に、アクセス ポイント間のピンポンの量を減らすためのものです。範囲：2 ～ 4 dB。デフォルト：2 dB。
Adaptive Scan Threshold	クライアントが関連付けられているアクセス ポイントの RSSI 値を入力します。この値以下の場合にクライアントは指定された移行時間内に隣接するアクセス ポイントにローミングできる必要があります。このフィールドはまた、クライアントがアクティブまたはパッシブ スキャンで費やす時間を最小限に抑えるための節電方法も提供します。たとえば、クライアントは RSSI が閾値よりも高いときにはゆっくりとスキャンし、閾値よりも低いときにはより速くスキャンすることができます。範囲：-70 ～ -77 dB。デフォルト：-72 dB。 **注**　[Scan Threshold] パラメータと [Transition Time] パラメータは、クライアントのローミング パフォーマンスの最低レベルを保証します。これらのパラメータと、最も高いクライアント速度とローミング ヒステリシスを一緒に使用すると、アクセス ポイント間に一定の最小オーバーラップ距離を確保することにより、ローミングをサポートする無線 LAN ネットワークを設計することが可能となります。
Transition Time	クライアントが関連付けられているアクセス ポイントの RSSI がスキャンしきい値を下回ったときに、クライアントがローミングする適切な隣接アクセス ポイントを検出し、ローミングを完了するまでの最大許容時間を入力します。範囲は 1 ～ 10 秒です。デフォルト：5 秒 **注**　[Scan Threshold] パラメータと [Transition Time] パラメータは、クライアントのローミング パフォーマンスの最低レベルを保証します。これらのパラメータと、最も高いクライアント速度とローミング ヒステリシスを一緒に使用すると、アクセス ポイント間に一定の最小オーバーラップ距離を確保することにより、ローミングをサポートする無線 LAN ネットワークを設計することが可能となります。

[Controller] > [80211b or g or n]

次に、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [80211b or g or n] にあるページの各フィールドについて説明します。

- [Controller] > [802.11b or g or n] > [dot11b-RRM] > [DCA]（2-27 ページ）
- [Controller] > [802.11b or g or n] > [dot11b-RRM] > [Intervals]（2-27 ページ）

- [Controller] > [802.11b or g or n] > [dot11b-RRM] > [Thresholds]（2-27 ページ）
- [Controller] > [802.11b or g or n] > [dot11b-RRM] > [TPC]（2-27 ページ）
- [Controller] > [802.11b or g or n] > [CleanAir]（2-27 ページ）
- [Controller] > [802.11b or g or n] > [EDCA Parameters]（2-27 ページ）
- [Controller] > [802.11b or g or n] > [High Throughput (802.11n)]（2-28 ページ）
- [Controller] > [802.11b or g or n] > [Media Parameters]（2-28 ページ）
- [Controller] > [802.11b or g or n] > [Parameters]（2-30 ページ）
- [Controller] > [802.11b or g or n] > [Roaming Parameters]（2-33 ページ）

[Controller] > [802.11b or g or n] > [dot11b-RRM] > [DCA]

[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [802.11b or g or n] > [dot11b-RRM] > [DCA] のフィールドの説明については、「[Controller] > [80211a or n or ac] > [dot11a-RRM] > [DCA]（2-17 ページ）」を参照してください。

[Controller] > [802.11b or g or n] > [dot11b-RRM] > [Intervals]

[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [802.11b or g or n] > [dot11b-RRM] > [Intervals] のフィールドの説明については、「[Controller] > [80211a or n or ac] > [dot11a-RRM] > [Intervals]（2-18 ページ）」を参照してください。

[Controller] > [802.11b or g or n] > [dot11b-RRM] > [TPC]

[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [802.11b or g or n] > [dot11b-RRM] > [TPC] のフィールドの説明については、「[Controller] > [80211a or n or ac] > [dot11a-RRM] > [TPC]（2-18 ページ）」を参照してください。

[Controller] > [802.11b or g or n] > [dot11b-RRM] > [Thresholds]

[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [802.11b or g or n] > [dot11b-RRM] > [Thresholds] のフィールドの説明については、「[Controller] > [80211a or n or ac] > [dot11a-RRM] > [Thresholds]（2-19 ページ）」を参照してください。

[Controller] > [802.11b or g or n] > [CleanAir]

[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [802.11b or g or n] > [CleanAir] の各フィールドの説明については、「[Controller] > [80211a or n or ac] > [CleanAir]（2-20 ページ）」を参照してください。

[Controller] > [802.11b or g or n] > [EDCA Parameters]

このオプションを使用して、802.11b/g/n EDCA パラメータを設定するテンプレートを作成または変更します。EDCA パラメータは、音声およびビデオの MAC レイヤで事前設定プロファイルを指定します。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [802.11b or g or n] > [EDCA Parameters] にある [Template Detail] の各フィールドについて説明します。

表 2-29　[Controller]> [80211b or g or n] > [EDCA Parameters]

フィールド	説明
EDCA Profile	プロファイルには、Wi-Fi Multimedia (WMM)、Spectralink Voice Priority (SVP)、Voice Optimized、および Voice & Video Optimized が含まれます。WMM がデフォルトの EDCA プロファイルです。 **注**　無線インターフェイスをシャットダウンしてから、EDCA パラメータを設定してください。 **注**　デバイスの WMM から WMM を無効にしたり、EDCA プロファイルを変更したりすると、AP の再起動時に 11n のレートが無効になります。
Low Latency MAC	このオプションは DSCP マーキングがメディア(RTP)およびシグナリング パケットに適切な場合にのみ有効にします。

[Controller] > [802.11b or g or n] > [High Throughput (802.11n)]

このオプションを使用して、MCS(データ レート)設定およびインデックスなどのハイ スループット パラメータを設定し、これらの 802.11n 設定を複数のコントローラに適用するテンプレートを作成または変更します。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [802.11b or g or n] > [High Throughput (802.11n)] にある [Template Detail] の各フィールドについて説明します。

表 2-30　[Controller] > [80211b or g or n] > [High Throughput (802.11n)]

フィールド	説明
802.11n Network Status	ハイ スループットを有効にするには、このチェックボックスをオンにします。
MCS (Data Rate) Settings	サポートするデータ レートのレベルを選択します。MCS は、802.11a データ レートと似た変調符号化方式です。デフォルトの値としては、20 MHz およびショート ガード インターバルが使用されます。[Supported] チェックボックスをオンにすると、選択した数値が [Selected MCS Indexes] ページに表示されます。

[Controller] > [802.11b or g or n] > [Media Parameters]

このオプションを使用して、コール アドミッション制御およびトラフィック ストリーム メトリックなど 802.11b/g/n の音声パラメータを設定するテンプレートを作成または変更します。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [802.11b or g or n] > [Media Parameters] にある [Template Detail] の各フィールドについて説明します。

表 2-31　[Controller]> [80211b or g or n] > [Media Parameters]

フィールド	説明
General	
Maximum Media Bandwidth (0 to 85%)	許容する最大帯域幅のパーセンテージを指定します。このオプションは、CAC が有効の場合のみ使用可能です。

表 2-31　[Controller]> [80211b or g or n] > [Media Parameters]（続き）

フィールド	説明
Video	
Admission Control (ACM)	アドミッション コントロールを有効にするには、このチェック ボックスをオンにします。
Maximum Bandwidth	許容する最大帯域幅のパーセンテージを指定します。このオプションは、CAC が有効の場合のみ使用可能です。
Reserved Roaming Bandwidth	予約するローミング帯域幅のパーセンテージを指定します。このオプションは、CAC が有効の場合のみ使用可能です。
Unicast Video Redirect	ビデオ キュー内のすべての非メディア ストリーム パケットがベスト エフォート キューにリダイレクトされるようにするには、[Unicast Video Redirect] チェックボックスをオンにします。無効にすると、ビデオ マーキングのあるパケットはすべてのビデオ キューに保持されます。
Client Minimum Phy Rate	クライアントがメディア ストリームに加入するために必要な物理データ レートを [Client Minimum Phy Rate] ドロップダウン リストから選択します。
Multicast Direct Enable	この無線上の任意の WLAN で Media Direct を有効にするには、[Multicast Direct Enable] チェックボックスを選択します。
Maximum Number of Streams per Radio	許容する無線ごとのストリームの最大数を指定します。
Maximum Number of Streams per Client	許容するクライアントごとのストリームの最大数を指定します。
Best Effort QOS Admission	新しいクライアント要求をベスト エフォート キューにリダイレクトするには、[Best Effort QOS Admission] チェックボックスをオンにします。これは、すべてのビデオ帯域幅が使用されている場合のみ発生します。無効になっており、最大のビデオ帯域幅が使用されている場合、新しいクライアント要求は拒否されます。
Voice	
Admission Control (ACM)	アドミッション コントロールを有効にするには、このチェック ボックスをオンにします。VoIP 通話中にエンド ユーザが許容できる音声品質と感じるよう、パケットはエンドポイントから別のエンドポイントまで低遅延、低パケット損失で配送される必要があります。異なるネットワーク負荷の下で QoS を維持するには、コール アドミッション制御（CAC）が必要です。アクセス時の CAC は、ネットワークのが輻輳していても CoS が維持された状態を保ち、許容する最大コール数を許容数に保つことができます。
CAC Method	[Admission Control (ACM)] が有効になっている場合は、CAC 方式を負荷ベースまたはスタティックに指定します。負荷ベースの CAC で取り入れられている測定方式では、それ自体からのすべてのトラフィック タイプによって同一チャネル アクセス ポイントで消費される帯域幅や、同一チャネルの干渉によって消費される帯域幅が考慮されています。load-based の CAC では、PHY およびチャネル欠陥の結果発生する追加の帯域幅消費も対象となります。
Maximum Bandwidth Allowed	許容する最大帯域幅のパーセンテージを入力します。このオプションは、CAC が有効の場合のみ使用可能です。
Reserved Roaming Bandwidth	予約するローミング帯域幅のパーセンテージを入力します。このオプションは、CAC が有効の場合のみ使用可能です。

表 2-31　[Controller]> [80211b or g or n] > [Media Parameters]（続き）

フィールド	説明
Expedited Bandwidth	緊急コール用に CAC の拡張として優先帯域幅を有効にするには、このチェックボックスを選択します。より高い優先度が TSPEC 要求に与えられるように、CCXv5 準拠の優先帯域幅の IE が必要となります。
SIP CAC	SIP CAC を有効にするには、このチェックボックスをオンにします。SIP CAC は、ステータス コード 17 をサポートし、TSPEC ベースのアドミッション制御をサポートしない電話のみに使用する必要があります。
SIP Codec	[SIP Codec] ドロップダウン リストから、この無線で使用するコーデック名を選択します。使用可能なオプションは、[G.711]、[G.729]、および [User Defined] です。
SIP Call Bandwidth	ネットワークで SIP コールごとに割り当てる帯域幅（キロビット/秒単位）を入力します。このフィールドは、選択されている [SIP Codec] が [User Defined] である場合のみ設定できます。
SIP Sample Interval	コーデックを動作させる必要があるサンプル間隔（ミリ秒）を入力します。
Max Number of Calls per Radio	無線ごとのコールの最大数を入力します。
Metric Collection	メトリック収集を有効にするには、このチェックボックスをオンにします。トラフィック ストリーム メトリックは、ワイヤレス LAN での VoIP に関する一連の統計情報で、ワイヤレス LAN の QoS を通知します。アクセス ポイントで測定値を収集するには、トラフィック ストリーム メトリックが有効であることが必要です。これを有効にすると、コントローラは、関連付けられたすべてのアクセス ポイントから、90 秒ごとに 802.11b/g インターフェイスに関する統計情報データの収集を開始します。VoIP またはビデオを使用している場合は、この機能を有効にする必要があります。

[Controller] > [802.11b or g or n] > [Parameters]

このオプションを使用して、802.11b/g/n パラメータ（電源およびチャネル ステータス、データレート、チャネル リストおよび CCX 位置測定など）を設定するテンプレートを作成または変更して、これらの設定をコントローラに適用します。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [802.11b or g or n] > [Parameters] にある [Template Detail] の各フィールドについて説明します。

表 2-32　[Controller] > [802.11b or g or n] > [Parameters]

フィールド	説明
Policy Name	適用されているセキュリティ ポリシーの名前を入力します。
Beam Forming	ドロップダウン リストから [enable] または [disable] を選択します。ビーム フォーミングは、信号の送受信の方を制御するときに使用される一般的な信号処理技術です。
Transmitted Power Threshold	送信電力のしきい値を入力します。有効な範囲は -50 ～ -80 です。
Beacon Period	SSID がアクセス ポイントによりブロードキャストされるレート（ビーコン間隔）。有効な範囲は 100 ～ 600 ミリ秒です。

表 2-32　[Controller] > [802.11b or g or n] > [Parameters]（続き）

フィールド	説明
DTIM Period	配送数フィールドが 0 のトラフィック インジケータ メッセージ（TIM）要素を含むビーコン フレームの送信間に経過したビーコン間隔。この値は、ビーコン フレームの DTIM Period フィールドで送信されます。DTIM を追加したビーコンをクライアント デバイスが受信すると、通常は、保留中のパケットをチェックするためにクライアント デバイスが「再起動」します。DTIM の間隔が長くなると、クライアントのスリープ時間が長くなり、電力を節約できます。反対に、DTIM の間隔が短くなるとパケットの受信の遅延を抑えられますが、クライアントが頻繁に起動するためバッテリ残量が消費されます。 DTIM の間隔は、コントローラ バージョン 5.0.0.0 以降では使用できません。
Fragmentation Threshold	パケットを断片化する（1 ブロックではなく、いくつかの断片として送信する）サイズを指定します。通信状態の悪いエリアや電波干渉が非常に多いエリアでは、低い数値を設定します。デフォルト値は 2346 です。
802.11e Max Bandwidth	802.11e の最大帯域幅のパーセンテージ。デフォルト値は 100 です。
Dynamic Assignment	[Dynamic Assignment] ドロップダウン リストから、次の動的送信電力割り当てモードのいずれかを選択します。 • [Automatic]：送信電力は、この操作を許可するすべてのアクセス ポイントで定期的に更新されます。 • [On Demand]：送信電力は、[Assign Now] をクリックすると更新されます。 • [Disabled]：動的な送信電力の割り当ては行われず、値はグローバル デフォルトに設定されます。 デフォルトは Automatic です。電力レベルおよび使用可能なチャネルは国コード設定によって定義されており、国別に規制されています。
Dynamic Tx Power Control	DTPC サポートを有効にするには、このチェックボックスをオンにします。このオプションが有効な場合、無線の送信電力レベルは、ビーコンにアドバタイズされ、プローブが応答します。
Assignment Mode	[Assignment Mode] ドロップダウン リストから、次の動的チャネル割り当てモードのいずれかを選択します。 • [Automatic]：チャネル割り当ては、この操作を許可するすべてのアクセス ポイントで定期的に更新されます。 • [On Demand]：チャネル割り当ては、必要に応じて更新されます。 • [Disabled]：動的なチャネル割り当ては行われず、値はグローバル デフォルトに設定されます。 デフォルトは Automatic です。
Avoid Foreign AP	この無線リソース管理（RRM）外部 802.11 干渉モニタリング フィールドを有効にすると、シスコのアクセス ポイントにチャネルを割り当てるときに、無線リソース管理によって外部（RF/モビリティ ドメイン外のシスコ以外のアクセス ポイント）アクセス ポイントからの干渉が考慮されます。無線リソース管理にこの干渉を無視させるには、このフィールドを無効にします。 外部アクセス ポイントからの干渉エネルギー（dB）および負荷（使用率）が著しい特定の状況では、無線リソース管理は、この外部アクセス ポイントの近くのシスコのアクセス ポイントのこれらのチャネル（および場合により隣接チャネル）を回避するために、チャネル割り当てを調整することがあります。これにより、シスコの WLAN ソリューションのキャパシティが増加し、変動性が減少します。

表 2-32　[Controller] > [802.11b or g or n] > [Parameters]（続き）

フィールド	説明
Avoid Cisco AP Load	この無線リソース管理（RRM）帯域幅認識フィールドを有効にすると、チャネルをアクセス ポイントに割り当てる際に、各アクセス ポイントで使用されるトラフィック帯域幅がコントローラによって考慮されます。無線リソース管理にこの値を無視させるには、このフィールドを無効にします。 特定の状況でより高密度に展開されている場合、完全なチャネルの再使用を適切に作成するには、チャネルが十分に存在しないことがあります。このような状況で、無線リソース管理は、より大きなトラフィック負荷を伝送する AP に、より良い再使用パターンを割り当てることができます。
Avoid non 802.11 Noise	この無線リソース管理（RRM）のノイズ モニタリング フィールドを有効にすると、電子レンジや Bluetooth デバイスなど、アクセス ポイントでないソースからの干渉のあるチャネルが回避されます。無線リソース管理にこの干渉を無視させるには、このフィールドを無効にします。 802.11 以外のノイズ源からの干渉エネルギー（dB）が著しい特定の状況では、このノイズ源の近くのアクセス ポイントのこれらのチャネル（および場合により隣接チャネル）を回避するため、無線リソース管理がチャネル割り当てを調整することがあります。これにより、シスコの WLAN ソリューションのキャパシティが増加し、変動性が減少します。
Signal Strength Contribution	このチェックボックスは常にオンです（変更不可）。無線リソース管理（RRM）は常に、RF/モビリティ ドメイン内のすべてのアクセス ポイントの相対位置をモニタし、最適に近いチャネルの再使用を保証します。その結果、Cisco WLAN Solution キャパシティについては増加、チャネル相互および隣接チャネルの干渉については減少となります。
Data Rates	データ レート セットは、クライアントとコントローラ間でネゴシエートされます。データ レートが [Mandatory] に設定されている場合、クライアントはネットワークを使用するには、そのデータ レートをサポートしている必要があります。データ レートがコントローラで [Supported] として設定されている場合は、同じレートをサポートしており、関連付けられているクライアントはそのレートを使用してアクセス ポイントと通信する可能性があります。しかし、6、9、12、18、24、36、48、54 Mbps を関連付けるために、サポートされるすべてのレートをクライアントが使用する必要はありません。 それぞれのレートについて、[Mandatory] または [Supported] のドロップダウン リスト選択が可能です。各データ レートは、[Disabled] に設定し、クライアントの設定に合わせることもできます。
Channel List	必要なモニタリング レベルに基づいて、すべてのチャネル、カントリー チャネルまたは DCA チャネルを選択します。Dynamic Channel Allocation（DCA）により、コントローラに接続された管理対象デバイスの中から妥当なチャネルの割り当てが自動的に選択されます。
Mode	ブロードキャスト無線測定要求を有効または無効にします。有効にすると、このパラメータによってクライアントの位置の正確さが向上します。
Interval	測定要求間の秒単位の間隔です。 Cisco Compatible Extension 位置測定間隔は、測定モードが有効な場合だけ変更できます。

[Controller] > [802.11b or g or n] > [Roaming Parameters]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [802.11b or g or n] > [Roaming Parameters] にある [Template Detail] の各フィールドについて説明します。

表 2-33　[Controller] > [802.11b or g or n] > [Roaming Parameters]

フィールド	説明
Mode	ドロップダウン リストから [Default Values] または [Custom Values] を選択します。[Default Values] を選択した場合はローミング パラメータを使用できません。デフォルト値が表示されます。
Minimum RSSI	クライアントをアクセス ポイントに関連付けるときに必要な受信信号強度インジケータ（RSSI）の最小値を入力します。クライアントの平均の受信信号の強度がこの閾値より低い場合、通常、信頼できる通信はできません。したがって、最小の RSSI 値に達する前に、クライアントはより強い信号のある別のアクセス ポイントをすでに見つけてローミングしている必要があります。範囲：-80 ～ -90 dBm。デフォルト：-85 dBm。
Roaming Hysteresis	クライアントがローミングするために必要な隣接するアクセス ポイントの信号強度を示す値を入力します。このフィールドは、クライアントが物理的に 2 つのアクセス ポイントの境界上やその近くにある場合に、アクセス ポイント間のピンポンの量を減らすためのものです。範囲：2 ～ 4 dB。デフォルト：2 dB。
Adaptive Scan Threshold	クライアントが関連付けられたアクセス ポイントの RSSI 値を入力します。これ以下の場合、クライアントは指定された移行時間内に隣接するアクセス ポイントにローミングできる必要があります。このフィールドはまた、クライアントがアクティブまたはパッシブ スキャンで費やす時間を最小限に抑えるための節電方法も提供します。たとえば、クライアントは RSSI が閾値よりも高いときにはゆっくりとスキャンし、閾値よりも低いときにはより速くスキャンすることができます。範囲：-70 ～ -77 dB。デフォルト：-72 dB。 **注**　[Scan Threshold] パラメータと [Transition Time] パラメータは、クライアントのローミング パフォーマンスの最低レベルを保証します。これらのパラメータを使用すると、最も高いクライアント速度とローミング ヒステリシスが得られるだけでなく、アクセス ポイント間の一定の最小オーバーラップ距離を確保することにより、ローミングをサポートする無線 LAN ネットワークを設計することが可能となります。
Transition Time	クライアントが関連付けられたアクセス ポイントからの RSSI がスキャンのしきい値より低くなった場合に、クライアントがローミングに適した隣接するアクセス ポイントの検出およびローミングにかけられる最大許容時間を入力します。範囲は 1 ～ 10 秒です。デフォルト：5 秒 **注**　[Scan Threshold] パラメータと [Transition Time] パラメータは、クライアントのローミング パフォーマンスの最低レベルを保証します。これらのパラメータを使用すると、最も高いクライアント速度とローミング ヒステリシスが得られるだけでなく、アクセス ポイント間の一定の最小オーバーラップ距離を確保することにより、ローミングをサポートする無線 LAN ネットワークを設計することが可能となります。

[Controller] > [CLI] > [General]

このオプションを使用して、CLI コマンドのセットを含むテンプレートを作成し、それらを Prime Infrastructure から 1 つ以上のコントローラに適用できます。これらのテンプレートは、SNMP サポートまたはカスタム Prime Infrastructure ユーザ インターフェイスがない複数のコントローラに機能をプロビジョニングします。テンプレート コンテンツは、コマンド配列の文字列です。置換変数、条件式などはサポートされていません。

デバイスの CLI セッションは、ユーザ プリファレンスに基づいて確立されます。デフォルト プロトコルは SSH です。

注　コントローラで正しいユーザ名およびパスワードが設定されていても、ユーザ名およびパスワードが無効なため、Controller Telnet クレデンシャル チェックが失敗するか、コントローラ CLI テンプレートが失敗した場合、コントローラが CLI 接続の最大数を超えていないか確認してください。接続数が最大数を超えている場合、CLI セッションの最大数を増やすか、コントローラの既存の CLI セッションを終了してから、操作を再試行してください。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [CLI] > [General] にある [Template Detail] の各フィールドについて説明します。

表 2-34　[Controller] > [CLI] > [General]

フィールド	説明
Commands	一連の CLI コマンドを入力します。
Refresh Config after Apply	[Refresh Config after Apply] チェックボックスをオンにして、CLI テンプレートが正常に適用されたら、コントローラで refresh config を実行します。
Save Config to Flash after apply	設定を保存するには、[Save Config to Flash after apply] チェックボックスをオンにします。
Reboot Controller after apply	コントローラを再起動するには、[Reboot Controller after apply] チェックボックスをオンにします。
Ignore errors on Apply Template to Controllers	テンプレート適用中に発生したすべてのエラーを無視するには、[Ignore errors on Apply Template to Controllers] をオンにします。

[Controller] > [FlexConnect] > [FlexConnect AP Groups]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [FlexConnect] > [FlexConnect AP Groups] にある [Template Detail] の各フィールドについて説明します。

表 2-35　[Controller] > [FlexConnect] > [FlexConnect AP Groups]

フィールド	説明
General	
Primary RADIUS	この AP グループのプライマリ RADIUS 認証サーバ。RADIUS 認証サーバがコントローラ上にない場合は、Prime Infrastructure で設定した RADIUS サーバは適用されません。
Port Number	プライマリ RADIUS サーバのポート番号を入力します。
Shared Secret	テキスト ボックスに共有秘密を入力します。
Confirm Shared Secret	共有秘密を再入力します。
Secondary RADIUS	この AP グループのセカンダリ RADIUS 認証サーバ。RADIUS 認証サーバがコントローラ上にない場合は、Prime Infrastructure で設定した RADIUS サーバは適用されません。
Port Number	セカンダリ RADIUS サーバのポート番号を入力します。
Shared Secret	テキスト ボックスに共有秘密を入力します。
Confirm Shared Secret	共有秘密を再入力します。

表 2-35　[Controller] > [FlexConnect] > [FlexConnect AP Groups]（続き）

フィールド	説明
FlexConnect AP	アクセス ポイントのイーサネット MAC アドレスは、同じコントローラ上の複数の FlexConnect グループに存在できません。複数のグループが同じコントローラに適用されている場合は、[Ethernet MAC] チェックボックスをオンにして、グループの 1 つのアクセス ポイントの選択を解除します。この変更は保存したり、コントローラに適用したりできます。
FlexConnect Configuration	FlexConnect グループのローカル認証を有効にします。 **注**　[General] タブで、[Primary RADIUS Server] フィールドと [Secondary RADIUS Server] フィールドが [None] に設定されていることを確認します。
FlexConnect Local Authentication	この FlexConnect グループのローカル認証を有効にします。デフォルト値はオフです。 **注**　この機能を使用しようとすると、ライセンスの必要な機能であることを知らせる警告メッセージが表示されます。 **注**　ページ下部に表示される [Users configured in the group] リンクをクリックして、FlexConnect ユーザのリストを表示できます。FlexConnect ユーザを作成できるのは、FlexConnect AP Group を保存した後だけです。
EAP Type	FlexConnect アクセス ポイントで LEAP を使用してクライアントを認証できるようにします。 FlexConnect アクセス ポイントで EAP-FAST を使用してクライアントを認証できるようにするには、[EAP-FAST] チェックボックスをオンにします。手動の PAC プロビジョニングを使用するには、[EAP-FAST Key] テキスト ボックスと [Confirm EAP-FAST Key] テキスト ボックスに、PAC の暗号化と復号化に使用するキーを入力します。
Auto Key Generation	PAC プロビジョニング中に、PAC がないクライアントに PAC が自動的に送信されるようにします。
EAP-FAST Key	EAP-FAST サーバの権限識別子。識別子は 32 桁の 16 進数文字である必要があります。
EAP-FAST Authority ID	テキスト形式のローカル EAP-FAST サーバの権限識別子。32 桁までの 16 進数文字を入力できます。
EAP-FAST Authority Info	EAP-FAST サーバの権限情報を入力します。
EAP-FAST Pac Timeout	PAC が編集ボックスに表示される秒数を入力します。有効な範囲は 2 ～ 4095 秒です。
Image Upgrade	
FlexConnect AP Upgrade	FlexConnect アクセス ポイントをアップグレードする場合に選択します。
Slave Maximum Retry Count	スレーブが FlexConnect グループ内のマスターからのダウンロード開始を試行する最大回数。このオプションは、[FlexConnect AP Upgrade] チェックボックスをオンにした場合のみ使用できます。 **注**　[General] タブで [FlexConnect AP Upgrade] チェッ クボックスが有効になっている場合に限り、アクセス ポイントをマスター アクセス ポイントとして追加できます。
VLAN-ACL Mapping	このタブの編集テーブルを使用して VLAN-ACL マッピングを追加します。
VLAN ID	有効な VLAN ID の範囲は 1 ～ 4094 です。
Ingress ACL	入力 ACL を選択します。

表 2-35　[Controller] > [FlexConnect] > [FlexConnect AP Groups]（続き）

フィールド	説明
Egress ACL	出力 ACL を選択します。
WLAN-ACL Mapping	このタブの編集テーブルを使用して WLAN-ACL マッピングを追加します。
WLAN ID	WLAN ID。
WLAN Profile Name	WLAN プロファイルを選択します。
WebAuth ACL	WebAuth ACL を選択します。
Local Split	このタブの編集テーブルを使用してローカルスプリット ACL を追加または選択します。
WLAN Profile Name	WLAN プロファイルの名前をリストから選択します。
Local-Split ACL	ローカルスプリット ACL を選択します。
Web Policies	このタブの編集テーブルを使用してWeb ポリシーの ACL を追加または選択します。
Web-Policy ACL	Web ポリシー ACL を選択します。最大 16 個の Web-Policy ACL を追加できます。
Central DHCP	このタブの編集テーブルを使用して、各 WLAN プロファイルの中央 DHCP を追加または選択します。
WLAN Profile Name	WLAN プロファイルの名前をリストから選択します。
Central DHCP	このプロファイルの中央 DHCP を有効にするには [Enable] を選択します。
Override DNS	このプロファイルの DNS のオーバーライドを有効にするには [Enable] を選択します。
NAT-PAT	このプロファイルのネットワーク アドレスとポート アドレスの変換を有効にするには [Enable] を選択します。

[Controller] > [IPv6]

次に、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [IPv6] にあるページの各フィールドについて説明します。

- [Controller] > [IPv6] > [Neighbor Binding Timers]（2-36 ページ）
- [Controller] > [IPv6] > [RA Guard]（2-37 ページ）
- [Controller] > [IPv6] > [RA Throttle Policy]（2-37 ページ）

[Controller] > [IPv6] > [Neighbor Binding Timers]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [IPv6] > [Neighbor Binding Timers] にある [Template Detail] の各フィールドについて説明します。

表 2-36　[Controller] > [IPv6] > [Neighbor Binding Timers]

フィールド	説明
Down Lifetime Interval	このフィールドでダウン ライフタイムを有効にします。このチェックボックスをオンにした場合、[Down Lifetime Interval] テキスト ボックスに値を指定します。このダウン ライフタイム間隔は、ダウン インターフェイスから取得したエントリが削除されるまで、または、エントリが到達可能であるという証拠を受け取るまで、そのエントリがバインド テーブルに保持される最大時間（秒単位）を示します。範囲は 0 ～ 86400 秒で、デフォルト値は 0 です。
Reachable Lifetime Interval	このフィールドで到達可能ライフタイムを有効にします。このチェックボックスをオンにした場合、[Reachable Lifetime Interval] テキスト ボックスに値を指定します。到達可能ライフタイム間隔は、到達可能という証明（トラッキングを介した直接的な到達可能性、またはネイバー探索プロトコル（NDP）検査を介した間接的な到達可能性）を受け取らずにエントリが到達可能と見なされる最大時間（秒単位）を示します。この時間が経過すると、エントリはステイルに移行します。範囲は 0 ～ 86400 秒で、デフォルト値は 0 秒です。
Stale Lifetime Interval	このフィールドでステイル ライフタイムを有効にします。このチェックボックスをオンにした場合、[Stale Lifetime Interval] テキスト ボックスに値を指定します。ステイル ライフタイム間隔は、ステイル エントリが削除されるまで、または、ステイル エントリが到達可能であるという証拠を受け取るまで、そのエントリがバインド テーブルに保持される最大時間（秒単位）を示します。範囲は 0 ～ 86400 秒で、デフォルト値は 0 です。

[Controller] > [IPv6] > [RA Guard]

RA ガードは、RA をワイヤレス クライアントからドロップするときに使用される Unified Wireless ソリューションです。これはグローバルに設定され、デフォルトで有効です。IPv6 ルータ アドバタイズメント パラメータを設定するテンプレートを作成または変更できます。

[Controller] > [IPv6] > [RA Throttle Policy]

このオプションを使用して、ワイヤレス ネットワークで循環するマルチキャスト ルータ アドバタイズメント（RA）の量を制限します。RA スロット ポリシー、スロット期間およびその他のオプションなど IPv6 ルータ アドバタイズメント パラメータを設定するテンプレートを作成または変更できます。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [IPv6] > [RA Throttle Policy] にある [Template Detail] の各フィールドについて説明します。

表 2-37　[Controller] > [IPv6] > [RA Throttle Policy]

フィールド	説明
RA Throttle Policy	RA スロットル ポリシーを有効にします。
Throttle Period *<<存在しません>>*	秒単位のスロットル期間の長さ。値の範囲は 10 ～ 86400 秒です。
Max Through *<<存在しません>>*	秒単位での一定期間で通過する RA の数。
Interval Option *<<存在しません>>*	間隔オプションが指定されている RA の場合の動作を示します。

表 2-37　[Controller] > [IPv6] > [RA Throttle Policy]（続き）

フィールド	説明
Allow At-least *<<存在しません>>*	ルータ単位で抑制 *されない* RA の最小数を示します。
Allow At-most *<<存在しません>>*	ルータ単位で抑制 *されない* RA の最大数を示します。

[Controller] > [Location]

次に、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [Location] にあるページの各フィールドについて説明します。

- [Controller] > [Location] > [Location Configuration] > [General]（2-38 ページ）
- [Controller] > [Location] > [Location Configuration] > [Advanced]（2-39 ページ）

[Controller] > [Location] > [Location Configuration] > [General]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [Location] > [Location Configuration] > [General] にある [Template Detail] の各フィールドについて説明します。

表 2-38　[Controller] > [Location] > [Location Configuration] > [General]

フィールド	説明
RFID Tag Data Collection	タグ収集を有効にするには、このチェックボックスをオンにします。モビリティ サービス エンジンがコントローラからアセット タグ データを収集する前に、コントローラで **config rfid status enable** コマンドを使用して、アクティブ RFID タグの検出を有効にする必要があります。
Calibrating Client	このチェックボックスをオンにして、クライアントの校正を有効にします。コントローラは、アクセス ポイントから校正クライアントに通常の S36 または S60 要求を送信します（クライアント機能に異なります）。パケットは、すべてのチャネルで送信されます。チャネルに関係なくすべてのアクセス ポイント（チャネル変更なし）が、RSSI データを各位置のクライアントから収集します。これらの追加送信およびチャネル変更は、同時に発生する音声またはビデオ トラフィックの質が低下する場合があります。使用可能なすべての無線（802.11a/b/g/n）を使用するには、[Advanced] タブでマルチバンドを有効にする必要があります。
Normal Client	校正を行わないクライアントを使用するには、このチェックボックスをオンにします。S36 要求はクライアントに送信されません。S36 および S60 は、特定の Cisco Compatible Extensions との互換性があるクライアント ドライバです。S36 には CCXv2 以降との互換性があります。S60 には CCXv4 以降との互換性があります。詳細については『Cisco Context Aware and Location FAQ（シスコ コンテキスト認識およびロケーションに関する FAQ）』を参照してください。
Tags, Clients and Rogue APs/Clients	検出されたタグ、クライアント、不正 AP、または不正クライアントを通知するまでの時間を秒単位で指定します。
For Clients	クライアントの RSSI 測定が廃棄される時間を秒単位で入力します。
For Calibrating Clients	校正クライアントの RSSI 測定が廃棄される時間を秒単位で入力します。

表 2-38　[Controller] > [Location] > [Location Configuration] > [General]（続き）

フィールド	説明
For Tags	タグの RSSI 測定が廃棄される時間を秒単位で入力します。
For Rogue APs	不正アクセス ポイントの RSSI 測定が廃棄される時間を秒単位で入力します。

[Controller] > [Location] > [Location Configuration] > [Advanced]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [Location] > [Location Configuration] > [Advanced] にある [Template Detail] の各フィールドについて説明します。

表 2-39　[Controller] > [Location] > [Location Configuration] > [Advanced]

フィールド	説明
RFID Tag Data Timeout	RFID タグ データのタイムアウトを設定する秒単位の値を入力します。
Calibrating Client Multiband	すべてのチャネルで S36 および S60 パケット（該当する場合）を送信するには、このチェックボックスをオンにします。調整クライアントは、[General] タブで有効にする必要があります。

[Controller] > [Management]

次に、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [Management] にあるページの各フィールドについて説明します。

- [Controller] > [Management] > [Legacy Syslog]（2-39 ページ）
- [Controller] > [Management] > [Local Management User]（2-40 ページ）
- [Controller] > [Management] > [Trap Control]（2-41 ページ）
- [Controller] > [Management] > [Trap Receiver]（2-42 ページ）

[Controller] > [Management] > [Legacy Syslog]

注　レガシー syslog は、5.0.6.0 以前のコントローラ バージョンに適用されます。

このテンプレートの作成に関する基本情報については、*『Cisco Prime Infrastructure 3.0 User Guide』*の「Creating Feature-Level Configuration Templates（機能レベルの設定テンプレートの作成）」を参照してください。

[Controller] > [Management] > [Local Management User]

このオプションを使用して、ローカル ユーザ、それらのユーザの特権レベルおよびパスワードを設定します。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [Management] > [General] にある [Template Detail] の各フィールドについて説明します。

表 2-40　[Controller] > [Management] > [Local Management User]

フィールド	説明
User Name	テンプレート ユーザ名を入力します。
Password	このローカル管理ユーザ テンプレートのパスワードを入力します。
Confirm Password	パスワードを再度入力します。
Access Level	[Access Level] ドロップダウン リストを使用して、[Read Only] または [Read Write] を選択します。
Update Telnet Credentials	Telnet/SSH アクセスの Prime Infrastructure のユーザ クレデンシャルを更新するには、[Update Telnet Credentials] チェックボックスをオンにします。 **注**　テンプレートが正常に適用され、[Update Telnet Credentials] オプションが有効な場合、適用される管理ユーザ クレデンシャルが、その適用コントロールへの Telnet/SSH クレデンシャルの Prime Infrastructure で使用されます。

[Controller] > [Management] > [Telnet SSH]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [Management] > [Telnet SSH] にある [Template Detail] の各フィールドについて説明します。

表 2-41　[Controller] > [Management] > [Telnet SSH]

フィールド	説明
Session Timeout	ログオフされるまでに Telnet セッションが非アクティブの状態を継続できる時間を分単位で入力します。0 は、タイムアウトしないことを意味します。有効な範囲は 0 ～ 160 で、デフォルトは 5 です。
Maximum Sessions	許可する同時 Telnet セッションの数を入力します。有効な範囲は 0 ～ 5 で、デフォルトは 5 です。DS（ネットワーク）ポートでは、新しい Telnet セッションを許可または禁止できます。サービス ポートでは、新しい Telnet セッションは常に許可されます。
Allow New Telnet Session	DS ポートでの新しい Telnet セッションを許可する場合は [Yes]、許可しない場合は [No] を選択します。DS（ネットワーク）ポートでは、新しい Telnet セッションを許可または禁止できます。サービス ポートでは、新しい Telnet セッションは常に許可されます。デフォルトは [Yes] です。
Allow New SSH Session	セキュア シェル Telnet セッションを許可する場合は [Yes]、許可しない場合は [No] を選択します。デフォルトは [Yes] です。

[Controller] > [Management] > [Trap Control]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [Management] > [Trap Control] にある [Template Detail] の各フィールドについて説明します。

表 2-42　[Controller] > [Management] > [Trap Control]

フィールド	説明
Select All Traps	このページのすべてのトラップを有効にするには、このチェックボックスをオンにします。
SNMP 認証	SNMPv2 エンティティが、適切に認証されていないプロトコル メッセージを受信しました。SNMP V3 モードで設定されているユーザが正しくないパスワードでコントローラにアクセスを試みると、認証は失敗し、エラー メッセージが表示されます。ただし、認証エラーの場合、トラップ ログは生成されません。
Link (Port) Up/Down	状態をアップまたはダウンに変更するには、[Link (Port) Up/Down] チェックボックスをオンにします。.
Multiple Users	同じログイン ID で 2 人のユーザがログインできるようにするには、[Multiple Users] チェックボックスをオンにします。
Spanning Tree	スパニング ツリーのトラップを有効にするには、[Spanning Tree] チェックボックスをオンにします。個々のパラメータの説明については、STP の仕様を参照してください。
Rogue AP	不正なアクセス ポイントが検出された場合や、以前に検出された不正なアクセス ポイントが存在しなくなった場合に、MAC アドレスを使用してトラップを送信するには、[Rogue AP] チェックボックスをオンにします。
Controller Config Save	設定を変更したときに通知を送信するには、[Controller Config Save] チェックボックスをオンにします。
802.11 Association	クライアントが WLAN に関連付けられたときにトラップを送信するには、[802.11 Association] をオンにします。このトラップは、クライアントが認証されることを保証しません。
802.11 Disassociation	クライアントが関連付け解除のフレームを送信したときに関連付け解除通知を送信するには、[802.11 Disassociation] チェックボックスをオンにします。
802.11 Deauthentication	クライアントが認証解除のフレームを送信したときに認証解除通知を送信するには、[802.11 Deauthentication] チェックボックスをオンにします。
802.11 Failed Authentication	クライアントが成功以外のステータス コードで認証フレームを送信したときに認証失敗通知を送信するには、[802.11 Failed Authentication] チェックボックスをオンにします。
802.11 Failed Association	クライアントが成功以外のステータス コードで関連付けフレームを送信したときに関連付け失敗通知を送信するには、[802.11 Failed Association] チェックボックスをオンにします。
除かれた	クライアントが除外されたときに関連付け失敗通知を送信するには、[Excluded] チェックボックスをオンにします。
AP Register	アクセス ポイントがコントローラに関連付けられたとき、またはコントローラとの関連付けが解除されたときに通知を送信するには、[AP Register] チェックボックスをオンにします。
AP Interface Up/Down	アクセス ポイント インターフェイス(802.11a/n または 802.11b/g/n)のステータスがアップまたはダウンになったときに通知を送信するには、[AP Interface Up/Down] チェックボックスをオンにします。

表 2-42　[Controller] > [Management] > [Trap Control]（続き）

フィールド	説明
Load Profile	負荷プロファイルの状態が PASS から FAIL、または FAIL から PASS に変化したときに通知を送信するには、[Load Profile] チェックボックスをオンにします。
Noise Profile	ノイズ プロファイルの状態が PASS から FAIL、または FAIL から PASS に変化したときに通知を送信するには、[Noise Profile] チェックボックスをオンにします。
Interference Profile	干渉プロファイルの状態が PASS から FAIL、または FAIL から PASS に変化したときに通知を送信するには、[Interference Profile] チェックボックスをオンにします。
Coverage Profile	カバレッジ プロファイルの状態が PASS から FAIL、または FAIL から PASS に変化したときに通知を送信するには、[Coverage Profile] チェックボックスをオンにします。
channel update	アクセス ポイントの動的チャネル アルゴリズムが更新されたときに通知を送信するには、[Channel Update] チェックボックスをオンにします。
Tx Power Update	アクセス ポイントの動的送信電力アルゴリズムが更新されたときに通知を送信するには、[Tx Power Update] チェックボックスをオンにします。
User Auth Failure	クライアントの RADIUS 認証の失敗が発生したときにトラップを送信してユーザに通知するには、[User Auth Failure] チェックボックスをオンにします。
RADIUS Server No Response	RADIUS クライアントが送信した認証要求に応答する RADIUS サーバがないことを示すためにトラップを送信するには、[RADIUS Server No Response] チェックボックスをオンにします。
ESP Authentication Failure	無効なハッシュがある IPsec パケットが着信 ESP SA で見つかったときに通知を送信するには、このチェックボックスをオンにします。
ESP Replay Failure	無効なシーケンス番号がある IPsec パケットが着信 ESP SA で見つかったときに通知を送信するには、[ESP Authentication Failure] チェックボックスをオンにします。
Invalid SPI	不明な SPI があるパケットが、指定したプロトコルを使用して指定した SPI がある指定したピアから検出されたときに通知を送信するには、[Invalid SPI] チェックボックスをオンにします。
IKE Negotiation Failure	フェーズ 1 IKE SA をネゴシエートする試行が失敗したときに通知を送信するには、[IKE Negotiation Failure] チェックボックスをオンにします。ネゴシエーション エラーの総数カウンタの現在の値とともに、トラップの一部として通知回数も送信されます。
IKE Suite Failure	指定したセレクタのフェーズ 2 SA スイートをネゴシエートする試行が失敗したときに通知を送信するには、[IKE Suite Failure] チェックボックスをオンにします。この障害に関係した通知の通知タイプ回数とともに、現在の合計障害回数が渡されます。
Invalid Cookie	指定された宛先への、無効な cookie がある ISAKMP パケットが指定された送信元から検出されたときに通知を送信するには、[Invalid Cookie] チェックボックスをオンにします。発信側と送信側の cookie もトラップとともに送信されます。
WEP Decrypt Error	コントローラが WEP 復号化エラーを検出したときに通知を送信するには、[WEP Decrypt Error] チェックボックスをオンにします。
Signature Attack	802.11 セキュリティ トラップを有効にするには、[Signature Attack] チェックボックスをオンにします。

[Controller] > [Management] > [Trap Receiver]

ネットワーク上に SNMP トラップを受信するモニタリング デバイスがある場合、このページを使用してトラップ レシーバ テンプレートを追加できます。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [Management] > [Trap Receiver] にある [Template Detail] の各フィールドについて説明します。

表 2-43　[Controller] > [Management] > [Trap Receiver]

フィールド	説明
IP Address	サーバの IP アドレスを入力します。
Admin Status	SNMP トラップをレシーバに送信する場合は、このチェックボックスをオンにして、管理者ステータスを有効にします。

[Controller] > [Mesh] > [Mesh Settings]

コントローラとの接続を確立するには、このオプションを使用してアクセス ポイントを設定します。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [Mesh] > [Mesh Settings] にある [Template Detail] の各フィールドについて説明します。

表 2-44　[Controller] > [Mesh] > [Mesh Settings]

フィールド	説明
RootAP to MeshAP Range	[Root AP to Mesh AP Range] はデフォルトで 12,000 フィートです。ルート アクセス ポイントとメッシュ アクセス ポイント間の適切な距離をフィート単位で入力します。このグローバル フィールドは、コントローラにアクセス ポイントが接続されるとすべてのアクセスポイントに適用され、ネットワーク内に存在するすべての既存のアクセス ポイントにも適用されます。
Client Access on Backhaul Link	[Client Access on Backhaul Link] チェックボックスは、デフォルトでオンになっていません。このオプションが有効の場合、メッシュ アクセス ポイントは 802.11a/n 無線クライアントと 802.11a/n バックホールを介してアソシエートできます。このクライアント アソシエーションは、ルートとメッシュ アクセス ポイント間の 802.11a/n バックホール上の既存の通信に追加されます。 **注**　この機能は 2 つの無線のあるアクセス ポイントだけに適用されます。
Background Scanning	バックグラウンド スキャンを有効にする場合は [Background Scanning] チェックボックスをオンにし、この機能を無効にする場合はオフにします。デフォルト値は [disabled] です。バックグラウンド スキャンにより、Cisco Aironet 1510 アクセス ポイントは、より最適なパスと親を探すために、能動的に連続して別のネイバーがいるチャネルをモニタできます。
Mesh DCA Channels	[Mesh DCA Channels] チェックボックスは、デフォルトでオンになっていません。このオプションをオンにして、コントローラで設定されている DCA チャネル リストを使用したコントローラでのバックホール チャネル選択解除を有効にします。コントローラ DCA リスト内のチャネルに対する変更はすべて、関連付けられたアクセス ポイントに適用されます。この機能は、1524SB メッシュ アクセス ポイントだけに適用されます。この機能の詳細については、『*Controller Configuration Guide*』を参照してください。
Global Public Safety	グローバルなパブリック セーフティを確立するには、[Global Public Safety] チェックボックスをオンにします。
Security Mode	[Security Mode] ドロップダウン リストから、[EAP]（Extensible Authentication Protocol）または [PSK]（事前共有キー）を選択します。

[Controller] > [PMIP]

プロキシ モバイル IPv6 は、任意の IP モビリティ関連シグナリングでモバイル ノードのプロキシとして動作することによってモバイル ノードをサポートする、ネットワーク ベースのモバイル管理プロトコルです。ネットワークのモビリティ エンティティは、モバイル ノードの移動を追跡し、モビリティ シグナリングを起動して必要なルーティング状態を設定します。

主要な機能エンティティは Local Mobility Anchor（LMA）とモバイル アクセス ゲートウェイ（MAG）です。LMA はモバイル ノードの到達可能性状態を維持し、モバイル ノードの IP アドレス用のトポロジ アンカー ポイントです。MAG はモバイル ノードの代わりにモビリティ管理を行います。MAG はモバイル ノードがアンカーされているアクセス リンクに存在します。コントローラは MAG 機能を実装します。

次に、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [PMIP] にあるページの各フィールドについて説明します。

- [Controller] > [PMIP] > [Global Config]（2-44 ページ）
- [Controller] > [PMIP] > [LMA Config]（2-45 ページ）
- [Controller] > [PMIP] > [PMIP Profile]（2-45 ページ）

[Controller] > [PMIP] > [Global Config]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [PMIP] > [Global Config] にある [Template Detail] の各フィールドについて説明します。

表 2-45　[Controller] > [PMIP] > [Global Config]

フィールド	説明
Domain Name	ドメインの名前。
Maximum Bindings Allowed	コントローラが MAG に送信できるバインディング アップデートの最大数。有効な範囲は 0 ～ 40000 です。
Binding Lifetime	コントローラのバインディング エントリのライフタイム。有効な範囲は 10 ～ 65535 秒です。デフォルト値は 65535 です。バインディング ライフタイムは 4 秒の倍数であることが必要です。
Binding Refresh Time	コントローラのバインディング エントリのリフレッシュ時間。有効な範囲は 4 ～ 65535 秒です。デフォルト値は 300 秒です。バインディング リフレッシュ時間は 4 秒の倍数であることが必要です。
Binding Initial Retry Timeout	コントローラがプロキシ バインディング確認（PBA）を受信しない場合のプロキシ バインディング アップデート（PBU）間の初期タイムアウト。有効な範囲は 100 ～ 65535 秒です。デフォルト値は 1000 秒です。
Binding Maximum Retry Timeout	コントローラがプロキシ バインディング確認（PBA）を受信しない場合のプロキシ バインディング アップデート（PBU）間の最大タイムアウト。有効な範囲は 100 ～ 65535 秒です。デフォルト値は 32000 秒です。
Replay Protection Timestamp	受信したプロキシ バインディング確認のタイムスタンプと現在の日時との時間差の上限。有効な範囲は 1 ～ 255 ミリ秒です。デフォルト値は 7 ミリ秒です。
Minimum BRI Retransmit Timeout	コントローラが BRI メッセージを再送信するまでに待機する時間の最小値。有効な範囲は 500 ～ 65535 秒です。

表 2-45　[Controller] > [PMIP] > [Global Config]（続き）

フィールド	説明
Maximum BRI Retransmit Timeout	コントローラが Binding Revocation Indication（BRI）メッセージを再送信するまでに待機する時間の最大値。有効な範囲は 500 ～ 65535 秒です。デフォルト値は 2000 秒です。
BRI Retries	コントローラが Binding Revocation Acknowledgment（BRA）メッセージを受信する前に BRI メッセージを再送信する最大回数。有効な範囲は 1 ～ 10 です。デフォルト値は 1 です。

[Controller] > [PMIP] > [LMA Config]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [PMIP] > [LMA Config] にある [Template Detail] の各フィールドについて説明します。

表 2-46　[Controller] > [PMIP] > [LMA Config]

フィールド	説明
LMA Name	コントローラに接続された LMA の名前。
LMA IP Address	コントローラに接続された LMA の IP アドレス。

[Controller] > [PMIP] > [PMIP Profile]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [PMIP] > [PMIP Profile] にある [Template Detail] の各フィールドについて説明します。

表 2-47　[Controller] > [PMIP] > [PMIP Profile]

フィールド	説明
PMIP Profile	プロファイル名を入力し、[Add] をクリックします。
Network Access Identifier	プロファイルに関連付けられたネットワーク アクセス識別子（NAI）の名前。
LMA Name	プロファイルを関連付ける LMA の名前。
Access Point Node	コントローラに接続されているアクセス ポイント ノードの名前。

[Controller] > [Security]

次に、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [Security] にあるページの各フィールドについて説明します。

- [Controller] > [Security] > [AAA] > [RADIUS Auth Servers]（2-47 ページ）
- [Controller] > [Security] > [AAA] > [TACACS+ Servers]（2-50 ページ）
- [Controller > [Security] > [Local EAP] > [EAP-FAST Parameters]（2-51 ページ）
- [Controller] > [Security] > [Local EAP] > [General - Local EAP]（2-51 ページ）
- [Controller] > [Security] > [Local EAP] > [Local EAP Profiles]（2-52 ページ）
- [Controller] > [Security] > [Wireless Protection Policies] > [Ignored Rogue AP]（2-54 ページ）
- [Controller] > [Security] > [Wireless Protection Policies] > [Rogue AP Rules]（2-55 ページ）

- [Controller] > [Security] > [Wireless Protection Policies] > [Rogue Policies](2-56 ページ)
- [Controller] > [Security] > [Access Control Lists](2-57 ページ)
- [Controller] > [Security] > [CPU Access Control List](2-57 ページ)
- [Controller] > [Security] > [File Encryption](2-58 ページ)
- [Controller] > [Security] > [IPv6 Groups](2-58 ページ)

[Controller] > [Security] > [AAA] > [LDAP Servers]

この項では、Lightweight Directory Access Protocol(LDAP)サーバを、RADIUS データベースやローカル ユーザ データベースに類似したバックエンド データベースとして設定する方法について説明します。LDAP バックエンド データベースを使用すると、コントローラで、特定のユーザの資格情報(ユーザ名およびパスワード)を LDAP サーバから検索できるようになります。これらの資格情報は、ユーザの認証に使用されます。たとえば、ローカル EAP では、ユーザ クレデンシャルを取得するために、バックエンド データベースとして LDAP サーバを使用する場合があります。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [Security] > [AAA] > [LDAP Servers] にある [Template Detail] の各フィールドについて説明します。

表 2-48　[Controller] > [Security] > [AAA] > [LDAP Servers]

フィールド	説明
Server Address	サーバの IP アドレスを入力します。
Port Number	アクセス ポイントが接続されているコントローラのポート番号。
Bind Type	[Authenticated] または [Anonymous] を選択します。[Authenticated] を選択した場合、バインド ユーザ名およびパスワードも入力する必要があります。バインドは、検索処理を実行する空きソケットです。匿名のバインド要求は拒否されます。
Server User Base DN	ユーザすべてのリストを含む LDAP サーバ内のサブツリーの識別名を入力します。
Server User Attribute	LDAP サーバにユーザ名が含まれている属性を入力します。
Server User Type	ユーザを識別する ObjectType 属性を入力します。
Retransmit Timeout	再送信の間隔を秒単位で入力します。有効な範囲は 2 ～ 30 秒で、デフォルト値は 2 秒です。
Admin Status	LDAP サーバに管理権限を持たせる場合は、[Enable] チェックボックスをオンにします。

[Controller] > [Security] > [AAA] > [RADIUS Acct Servers]

このページでは、新しい RADIUS アカウンティング テンプレートの追加、または既存の RADIUS アカウンティング テンプレートの変更が可能です。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [Security] > [AAA] > [RADIUS Acct Servers] にある [Template Detail] の各フィールドについて説明します。

表 2-49　[Controller] > [Security] > [AAA] > [RADIUS Acct Servers]

フィールド	説明
Server Address	サーバ アドレスを入力します。
Port Number	ポート アドレスを入力します。
Shared Secret Format	[ASCII] または [Hex] を選択します。 **注**　選択した形式に関係なく、セキュリティ上の理由で、ASCII のみが ワイヤレス LAN コントローラ（および Prime Infrastructure）に表示されます。そのため、自動プロビジョニング時にテンプレートを使用しても、別のコントローラの設定を複製できません。検出されたテンプレートが別のデバイスに適用される場合、テンプレートでもう一度キー形式を設定する必要があります。
Shared Secret Confirm Shared Secret	指定したサーバで使用する RADIUS 共有秘密を入力し、確認します。
Admin Status	サーバに管理権限を確立する場合は、[Enable] チェックボックスをオンにします。
Network User	ネットワーク ユーザ認証を有効にする場合はオンにします。このオプションが有効な場合、このエントリがネットワーク ユーザの RADIUS 認証サーバと見なされます。
Retransmit Timeout	RADIUS 認証要求がタイムアウトし、コントローラが再転送を試みるまでの時間を秒単位で指定します。2 ～ 30 秒の値を指定できます。
IPsec Enable	IP セキュリティ を有効にするには、[Enable] チェックボックスをオンにします。

[Controller] > [Security] > [AAA] > [RADIUS Auth Servers]

このオプションを使用して、RADIUS 認証テンプレートを追加するか、または既存のテンプレートを変更します。これらのサーバ テンプレートを設定した後、CLI または GUI を経由してコントローラにログインしているコントローラ ユーザが認証されます。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [Security] > [AAA] > [RADIUS Auth Servers] にある [Template Detail] の各フィールドについて説明します。

表 2-50　[Controller] > [Security] > [AAA] > [RADIUS Auth Servers]

フィールド	説明
Server Address	サーバ アドレスを入力します。
Port Number	ポート アドレスを入力します。

表 2-50　[Controller] > [Security] > [AAA] > [RADIUS Auth Servers]（続き）

フィールド	説明
Shared Secret Format	[ASCII] または [hex] を選択します。 **注**　選択した形式に関係なく、セキュリティ上の理由で、ASCII のみが WLC（および Prime Infrastructure）に表示されます。そのため、自動プロビジョニング時にテンプレートを使用しても、別のコントローラの設定を複製できません。検出されたテンプレートが別のデバイスに適用される場合、テンプレートでもう一度キー形式を設定する必要があります。
Shared Secret	指定のサーバで使用する RADIUS 共有秘密を入力します。
Confirm Shared Secret	指定のサーバで使用する RADIUS 共有秘密を再入力します。
Key WRAP	キー ラップを有効にする場合は、チェックボックスをオンにします。このチェックボックスが有効な場合、認証要求は次の Key Encryption Key（KEK）および Message Authenticator Code Keys（MACK）が設定されている RADIUS サーバに送信されます。有効にされている場合、次のフィールドが表示されます。 • [Shared Secret Format]：ASCII または 16 進数を入力します。 **注**　選択した形式に関係なく、セキュリティ上の理由で、ASCII のみが WLC（および Prime Infrastructure）に表示されます。そのため、自動プロビジョニング時にテンプレートを使用しても、別のコントローラの設定を複製できません。検出されたテンプレートが別のデバイスに適用される場合、テンプレートでもう一度キー形式を設定する必要があります。 • [KEK Shared Secret]：KEK 共有秘密を入力します。 • [MACK Shared Secret]：MACK 共有秘密を入力します。 **注**　コントローラが共有秘密の通知を受けるたびに、既存の共有秘密は新しい共有秘密に上書きされます。
Admin Status	管理権限を有効にする場合はオンにします。
Support for RFC 3576	RFC 3576 のサポートを有効にする場合はオンにします。RFC 3576 は、Remote Authentication Dial In User Service（RADIUS）プロトコルの拡張版です。これは、ユーザ セッションに対する動的な変更を可能とし、ユーザの接続解除やユーザ セッションに適用できる認可の変更に対するサポートを含みます。これらの認可と共に、[Disconnect] および [Change-of-Authorization]（CoA）メッセージのサポートが提供されます。[Disconnect] メッセージはユーザ セッションをただちに終了させ、CoA メッセージはデータ フィルタなどセッションの認可属性を変更します。
Network User	ネットワーク ユーザ認証を有効にする場合はオンにします。このオプションが有効な場合、このエントリがネットワーク ユーザの RADIUS 認証サーバと見なされます。
Management User	管理認証を有効にする場合はオンにします。このオプションが有効な場合、このエントリが管理ユーザの RADIUS 認証サーバと見なされます。
Retransmit Timeout	RADIUS 認証要求がタイムアウトし、コントローラが再転送を試みるまでの時間を秒単位で指定します。2 ～ 30 秒の値を指定できます。
IPSec	クリックして IP セキュリティ メカニズムを有効にすると、追加の IP セキュリティ フィールドがページに追加さます。

表 2-50　[Controller] > [Security] > [AAA] > [RADIUS Auth Servers]（続き）

フィールド	説明
IPsec Authentication	使用する IP セキュリティ認証プロトコルを選択します。オプションは、[HMAC-SHA1]、[HMAC-MD5]、および [None] です。 秘密キーを共有する 2 者間では、やり取りされる情報を検証するために、メッセージ認証コード（MAC）が使用されます。HMAC（ハッシュ MAC）は、暗号ハッシュ関数に基づいたメカニズムで、反復された任意の暗号ハッシュ関数の組み合わせで使用できます。HMAC-MD5 と HMAC-SHA1 は、MD5 ハッシュ関数と SHA1 ハッシュ関数を使用した HMAC の 2 つの構造です。また、HMAC では、メッセージ認証値の計算と検証に秘密キーを使用します。
IPsec Encryption	使用する IP セキュリティ暗号化メカニズムを選択します。 • DES：データ暗号規格（DES）は、秘密キーを使用してデータを暗号化する方法です。DES では、56 ビットのキーを 64 ビットのデータ ブロックごとに適用します。 • [Triple DES]：3 つのキーを連続で適用するデータ暗号規格。 • [AES 128 CBC]：高度暗号化規格（AES）は 128、192、または 256 ビットの長さのキーを使用して 128、192、または 256 ビットの長さのブロックを暗号化します。AES 128 CBC では、暗号ブロック連鎖（CBC）モードで 128 ビットのデータ パスを使用します。 • [None]：IP セキュリティ暗号化メカニズムはありません。
IKE Authentication	インターネット キー エクスチャンジ（IKE）認証は、編集可能なテキスト ボックスではありません。Internet Key Exchange プロトコルは、セッション キー（暗号化と認証）を配信し、VPN エンドポイントにデータの保護方法に合意する方法を提供するメソッドです。IKE はセキュリティ アソシエーション（SA）のバンドルを各接続に割り当てることによって、接続を追跡します。
IKE Phase 1	[aggressive] または [main] のいずれかを選択します。これによって、IKE プロトコルが設定されます。IKE phase 1 は、IKE の保護方法をネゴシエートするために使用されます。Aggressive モードは、少ないパケットでより多くの情報を渡し、若干高速の接続になる利点がありますが、セキュリティ ゲートウェイの ID を暗号化せずに転送する欠点があります。
Lifetime	セッションの期限が切れるまでのタイムアウト間隔（秒単位）を設定します。
IKE Diffie Hellman Group	IKE Diffie-Hellman グループを設定します。オプションは、[group 1]（768 ビット）、[group 2]（1024 ビット）、または [group 5]（1536 ビット）です。Diffie-Hellman 技術は、対称キーを生成するために 2 つのデバイスによって使用されます。これによって、値を公に交換し、同じ対称キーを生成できます。 3 つのグループのすべてで従来の攻撃に対するセキュリティが確保されますが、キーのサイズが大きいことから、Group 5 の安全性がより高くなります。ただし、Group 1 ベースまたは Group 2 ベースのキーを使用した計算は、素数サイズがより小さいために、多少高速に実行される可能性があります。

[Controller] > [Security] > [AAA] > [TACACS+ Servers]

このオプションを使用して、TACACS+ サーバ テンプレートを追加するか、または既存の TACACS+ サーバ テンプレートを変更します。これらのサーバ テンプレートを設定した後、CLI または GUI を経由してコントローラにログインしているコントローラ ユーザが認証されます。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [Security] > [AAA] > [TACACS+ Servers] にある [Template Detail] の各フィールドについて説明します。

表 2-51　[Controller] > [Security] > [AAA] > [TACACS+ Servers]

フィールド	説明
Server Type	チェックボックスをオンにして、1 つ以上のサーバ タイプを選択します。次のサーバ タイプが使用可能です。 • [authentication]：ユーザ認証/承認用のサーバ • [authorization]：ユーザ承認のみを行うサーバ • [accounting]：RADIUS ユーザ アカウンティング用のサーバ
Server Address	サーバの IP アドレスを入力します。
Port Number	サーバのポート番号を入力します。デフォルトは 49 です。
Shared Secret Format	[ASCII] または [hex] を選択します。 選択した形式に関係なく、セキュリティ上の理由で、ASCII のみが WLC（および Prime Infrastructure）に表示されます。そのため、自動プロビジョニング時にテンプレートを使用しても、別のコントローラの設定を複製できません。検出されたテンプレートが別のデバイスに適用される場合、テンプレートでもう一度キー形式を設定します。
Shared Secret	指定のサーバで使用する TACACS+ 共有秘密を入力します。
Confirmed Shared Secret	指定のサーバで使用する TACACS+ 共有秘密を再入力します。
Admin Status	LDAP サーバに管理権限を持たせる場合はオンにします。
Retransmit Timeout	TACACS+ 認証要求がタイムアウトし、コントローラが再転送を試みるまでの時間を秒単位で入力します。

[Controller > [Security] > [Local EAP] > [EAP-FAST Parameters]

この認証のタイプ（Flexible Authentication via Secure Tunneling）は、3 段階のトンネル認証プロセスを使用して高度な 802.1X EAP 相互認証を実行します。ユーザ名、パスワード、および PAC を使用し、アクセス ポイントを介して RADIUS サーバと相互認証を行います。このページでは、EAP-FAST テンプレートの追加、または既存の EAP-FAST テンプレートの変更が可能です。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [Security] > [Local EAP] > [EAP-FAST Parameters] にある [Template Detail] の各フィールドについて説明します。

表 2-52　[Controller] > [Security] > [Local EAP] > [EAP_FAST Parameters]

フィールド	説明
Time to Live for the PAC	PAC の有効日数を入力します。有効な範囲は 1 ～ 1000 日で、デフォルトの設定は 10 日です。
Authority ID	16 進数文字のローカル EAP-FAST サーバの権限識別子を入力します。最大 32 文字の 16 進数文字を入力できますが、文字数は偶数である必要があります。
Authority Info	テキスト形式のローカル EAP-FAST サーバの権限識別子を入力します。
Server Key and Confirm Server Key	PAC の暗号化と復号化に使用するキー（16 進数文字）を入力します。
Anonymous Provision	匿名プロビジョニングを有効する場合にオンにします。この機能を使用すると、PAC プロビジョニング中に、PAC がないクライアントに PAC が自動的に送信されるようになります。この機能を無効にすると、PAC を手動でプロビジョニングする必要があります。

[Controller] > [Security] > [Local EAP] > [General - Local EAP]

このページでは、ローカル EAP のタイムアウト値を指定できます。次に、既存のローカル EAP 汎用テンプレートに変更を追加すること、またはこのテンプレートを変更することができます。

注　コントローラで RADIUS サーバが設定されている場合は、コントローラは最初に RADIUS サーバを使用してワイヤレス クライアントを認証しようとします。ローカル EAP は、RADIUS サーバがタイムアウトしていたり、RADIUS サーバが設定されていない場合など、RADIUS サーバが見つからない場合にのみ試行されます。4 台の RADIUS サーバが設定されている場合、コントローラは最初の RADIUS サーバを使用してクライアントの認証を試行し、次に 2 番めの RADIUS サーバ、その次にローカル EAP を試行します。その後クライアントが手動で再認証を試みると、コントローラは 3 番めの RADIUS サーバを試行し、次に 4 番めの RADIUS サーバ、その次にローカル EAP を試行します。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [Security] > [Local EAP] > [General - Local EAP] > にある [Template Detail] の各フィールドについて説明します。

表 2-53　[Controller] > [Security] > [Local EAP] > [General - Local EAP]

フィールド	説明
Local Auth Active Timeout	設定された RADIUS サーバのペアで障害が発生してから、コントローラがローカル EAP を使用してワイヤレス クライアントの認証を試みるまでの時間（秒単位）を入力します。有効な範囲は 1 ～ 3600 秒で、デフォルトの設定は 1000 秒です。
注　EAP-FAST、手動パスワード入力、ワンタイム パスワード、または 7920/7921 電話を使用する場合は、以下で指定した値を入力します。自動プロビジョニングを使用している PAC をクライアントで取得する場合、コントローラで 802.1x のタイムアウト値を大きくする必要があります（デフォルトは 2 秒）。Cisco ACS サーバでの推奨およびデフォルトのタイムアウトは 20 秒です。複数のコントローラで次の値が同じに設定されていないと、ローミングが失敗します。	
Local EAP Identity Request Timeout	1
Local EAP Identity Request Maximum Retries	20
Local EAP Dynamic WEP Key Index	0
Local EAP Request Timeout	20
Local EAP Request Maximum Retries	2
EAPOL-Key Timeout	1000（ミリ秒単位）
EAPOL-Key Max Retries	2
Max Login Ignore Identity Response	コントローラに同じユーザ名で接続できるデバイスの数を制限するには、[Enable] をオンにします。

[Controller] > [Security] > [Local EAP] > [Local EAP Profiles]

このページでは、ローカル EAP プロファイル テンプレートの追加、または既存のテンプレートの変更が可能です。ローカル EAP は、ユーザおよびワイヤレス クライアントのローカル認証を可能にする認証方式です。この方式は、バックエンド システムが妨害されたり、外部認証サーバがダウンした場合でも、ワイヤレス クライアントへの接続を維持できるように、リモート オフィスで使用する目的で設計されています。ローカル EAP を有効にすると、コントローラは認証サーバおよびローカル ユーザ データベースとして機能するため、外部認証サーバへの依存が排除されます。ローカル EAP は、ローカル ユーザ データベースまたは LDAP バックエンド データベースからユーザの資格情報を取得して、ユーザを認証します。

注　LDAP バックエンド データベースは、次のローカル EAP メソッドだけをサポートします。証明書による EAP-TLS および EAP-FAST。LDAP バックエンド データベースでは、LEAP および PAC による EAP-FAST はサポートされません。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [Security] > [Local EAP] > [Local EAP Profiles] にある [Template Detail] の各フィールドについて説明します。

表 2-54　[Controller] > [Security] > [Local EAP] > [Local EAP Profiles]

フィールド	説明
EAP Profile Name	ユーザ定義の識別子。
Select Profile Methods	目的の認証タイプを選択します。 • この認証のタイプは Cisco Key Integrity Protocol（CKIP）と Multi-Modal Hashing（MMH）メッセージ整合性チェック（MIC）を使用してデータを保護します。ユーザ名とパスワードを使用し、アクセス ポイントを介して RADIUS サーバと相互認証を行います。 • [EAP-FAST]：この認証のタイプ（Flexible Authentication via Secure Tunneling）は、3 段階のトンネル認証プロセスを使用して高度な 802.1X EAP 相互認証を実行します。ユーザ名、パスワード、および PAC（保護されたアクセス クレデンシャル）を使用し、アクセス ポイントを介して RADIUS サーバと相互認証を行います。 • [TLS]：この認証のタイプは、クライアント アダプタおよび RADIUS サーバの動的セッション ベースの暗号鍵を使用してデータを暗号化します。認証のためには、クライアント証明書が必要です。 • [PEAP]：この認証のタイプは EAP-TLS 認証に基づいていますが、認証にクライアント証明書ではなくパスワードを使用します。PEAP は、クライアント アダプタおよび RADIUS サーバの動的セッション ベースの暗号鍵を使用してデータを暗号化します。
Certificate Issuer	認証用の証明書をシスコが発行したか、別のベンダーが発行したかを特定します。証明書が必要なのは、EAP-FAST と TLS だけです。
Check Against CA Certificates	クライアントからの受信証明書をコントローラ上の認証局（CA）証明書と照合して検証する場合はオンにします。
Verify Certificate CN Identity	受信証明書の共通名（CM）を CA 証明書の共通名と照合して検証する場合はオンにします。
Check Against Date Validity	受信デバイス証明書がその時点でも有効で、期限が切れていないことをコントローラに確認させる場合はオンにします。
Local Certificate Required	ローカル証明書が必要な場合はオンにします。
Client Certificate Required	クライアント証明書が必要な場合はオンにします。

[Controller] > [Security] > [Wireless Protection Policies] > [Friendly Access Point]

このテンプレートを使用すると、危険性のない内部アクセス ポイントをインポートできます。危険性のないアクセス ポイントをインポートすると、非 Lightweight アクセス ポイントが不正アクセス ポイントとして識別されるのを防ぐことができます。

注　*危険性のない内部アクセス ポイントは、以前は既知の AP と呼ばれていました。*

[Friendly AP] ページでは、アクセス ポイントの MAC アドレス、ステータス、コメント、このアクセス ポイントに対するアラームの抑制有無が確認できます。

危険性のないアクセス ポイントは、アクセス ポイントをインポートするか、アクセス ポイント情報を手動で入力することにより追加できます。

- インポート機能を使用してアクセス ポイントをインポートする手順は次のとおりです。
  - [Import from File] チェックボックスをオンにします。
  - ファイルのパスを入力するか、[Browse] をクリックしてインポートするファイルを選択します。

注　改行を使用して、インポートするファイルの MAC アドレスを区切ります。たとえば、次のように、MAC アドレスを入力します。
00:00:11:22:33:44
00:00:11:22:33:45
00:00:11:22:33:46

- アクセス ポイントを手動で追加するには、次の手順に従います。

ステップ 1　[Import from File] チェックボックスをオフにします。

ステップ 2　アクセス ポイントの MAC アドレスを入力します。

ステップ 3　[Status] ドロップダウン リストから [Internal] アクセス ポイントを選択します。

ステップ 4　このアクセス ポイントに関するコメントを必要に応じて入力します。

ステップ 5　[Suppress Alarms] チェックボックスをオンにして、このアクセス ポイントのすべてのアラームを抑制します。

[Controller] > [Security] > [Wireless Protection Policies] > [Ignored Rogue AP]

[Ignored Rogue AP Template] ページでは、無視されるアクセス ポイントをインポートするテンプレートを作成または変更できます。[Ignored AP] リストのアクセス ポイントは、不正アクセス ポイントと識別されません。

無視される不正 AP テンプレートは、コントローラに適用されません。コントローラが不正 AP を Prime Infrastructure に報告するときに、無視される不正 AP テンプレートに不正 MAC アドレスがあり、この MAC アドレスがコントローラの不正 AP 無視リストに追加される場合、不正 AP/アドホック アラームが抑制されます。

無視される不正アクセス ポイントは、アクセス ポイントをインポートするか、アクセス ポイント情報を手動で入力することにより追加できます。

ステップ 1　インポート機能を使用して無視される不正アクセス ポイントをインポートする手順は、次のとおりです。<<インポート機能は存在しません>>

ステップ 2　[Import from File] チェックボックスをオンにします。<<存在しません>>

ステップ 3　ファイルのパスを入力するか、[Browse] ボタンを使用してインポートするファイルを選択します。インポート ファイルは、MAC アドレスを含む(1 行に MAC アドレス 1 つ)CSV ファイルにする必要があります。<<存在しません>>

注　たとえば、次のように、MAC アドレスを入力します。
00:00:11:22:33:44
00:00:11:22:33:45
00:00:11:22:33:46

無視された不正アクセス ポイントを手動で追加するには、[Import from File] チェックボックスをオフにします。<<存在しません>>

[Controller] > [Security] > [Wireless Protection Policies] > [Rogue AP Rules]

不正アクセス ポイントのルールを使用すると、不正アクセス ポイントを自動的に分類するルールを定義できます。Prime Infrastructure では、不正アクセス ポイントの分類ルールをコントローラに適用します。これらのルールでは、RSSI レベル（それよりも弱い不正アクセス ポイントは無視）、または時間制限（指定された時間内に表示されない不正アクセス ポイントにはフラグを立てない）に基づいて、マップ上の不正表示を制限できます。

不正アクセス ポイントのルールは、誤アラームを減らすのにも役立ちます。

不正クラスには以下の種類があります。

- [Malicious Rogue]：検出されたアクセス ポイントのうち、ユーザが定義した Malicious ルールに一致したアクセス ポイント、または危険性のない AP カテゴリから手動で移動されたアクセス ポイント。
- [Friendly Rogue]：既知、認識済み、または信頼できるアクセス ポイント、または検出されたアクセス ポイントのうち、ユーザが定義した Friendly ルールに該当するアクセス ポイント。
- [Unclassified Rogue]：検出されたアクセス ポイントのうち、Malicious ルールまたは Friendly ルールに該当しないアクセス ポイント。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [Security] > [Wireless Protection Policies] > [Rogue AP Rules] にある [Template Detail] の各フィールドについて説明します。

表 2-55　[Controller] > [Security] > [Wireless Protection Policies] > [Rogue AP Rules]

フィールド	説明
Rule Type	ドロップダウン リストから [Malicious] または [Friendly] を選択します。検出されたアクセス ポイントがユーザ定義の Malicious ルールと合致した場合、または危険性のない AP カテゴリから手動で移動された場合には、悪意のある不正と見なされます。不正が既知、認知済み、または信頼されたアクセス ポイントである場合、または検出されたアクセス ポイントがユーザ定義の Friendly ルールと一致している場合、危険性がない不正と見なされます。
Match Type	[Match All Conditions] または [Match Any Condition] を選択します。
Open Authentication	オープン認証を有効にするには、このチェックボックスをオンにします。
Match Managed AP SSID	管理対象 AP の SSID との一致を有効にするには、このチェックボックスをオンにします。 **注**　管理対象 SSID は、WLAN に対して設定された SSID で、システムが既知のものです。
Match User Configured SSID	ユーザ設定の SSID との一致を有効にするには、このチェックボックスをオンにします。 **注**　ユーザ設定の SSID は、手動で追加された SSID です。[Match User Configured SSID] テキスト ボックスに、ユーザ設定の 定義の SSID を（1 行に 1 つずつ）入力します。
Minimum RSSI	最小 RSSI しきい値制限を有効にするには、このチェックボックスをオンにします。 **注**　テキスト ボックスに RSSI 閾値の最小レベル（dB 単位）を入力します。検出されたアクセス ポイントがここで指定した RSSI 閾値を超えていると、そのアクセス ポイントは悪意のあるものとして分類されます。

表 2-55　[Controller] > [Security] > [Wireless Protection Policies] > [Rogue AP Rules]（続き）

フィールド	説明
Time Duration	時間制限を有効にするには、このチェックボックスをオンにします。 **注**　テキスト ボックスに制限時間（秒単位）を入力します。検出されたアクセス ポイントが指定した制限時間よりも長く表示されているとき、そのアクセス ポイントは悪意のあるものとして分類されます。
Minimum Number Rogue Clients	最小不正クライアント数制限を有効にするには、このチェックボックスをオンにします。悪意のあるクライアントを許可する最小数を入力します。検出されたアクセス ポイントにアソシエートされたクライアントの数が指定した値以上になると、そのアクセス ポイントは悪意のあるものとして分類されます。

[Controller] > [Security] > [Wireless Protection Policies] > [Rogue Policies]

このページでは、コントローラに適用される（アクセス ポイントとクライアントに対する）不正ポリシーを設定できます。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [Security] > [Wireless Protection Policies] > [Rogue Policies] にある [Template Detail] の各フィールドについて説明します。

表 2-56　[Controller] > [Security] > [Wireless Protection Policies] > [Rogue Policies]

フィールド	説明
Rogue Location Discovery Protocol	Rogue Location Discovery Protocol（RLDP）が企業の有線ネットワークに接続しているかどうかを判断します。次のいずれかを選択します。 • [Disable]：すべてのアクセス ポイント上で RLDP を無効にします。 • [All APs]：すべてのアクセス ポイント上で RLDP を有効にします。 • [Monitor Mode APs]：モニタ モードのアクセス ポイント上でのみ RLDP を有効にします。 **注**　RLDP が有効の場合、コントローラは管理対象のアクセス ポイントに対して、不正アクセス ポイントをアソシエートし、特殊なパケットをコントローラへ送信するよう指示します。コントローラがこのパケットを受信すると、不正アクセス ポイントが企業ネットワークに接続されます。この方法は、暗号化を有効にしていない不正アクセス ポイントに対して機能します。
Expiration Timeout for Rogue AP and Rogue Client Entries	不正アクセス ポイント エントリの期限切れタイムアウトを秒単位で入力します。
Rogue Detection Report Interval	AP からコントローラに不正検出レポートを送信する間隔を秒単位で入力します。有効な範囲は 10 ～ 300 秒で、デフォルト値は 10 秒です。この機能は、モニタ モードの AP のみに適用されます。
Rogue Detection Minimum RSSI	AP で検出するために不正に必要であり、かつコントローラで不正エントリが作成されるために必要な最小 RSSI 値を入力します。有効な範囲は -70 ～ -128 dBm で、デフォルト値は -128 dBm です。この機能は、すべての AP モードに適用できます。 非常に RSSI 値が低く、不正解析にとって有益な情報とならない不正が多く存在する可能性があります。そのため、このオプションを使用して AP が不正を検出する最小 RSSI 値を指定することで、不正をフィルタできます。

表 2-56　[Controller] > [Security] > [Wireless Protection Policies] > [Rogue Policies]（続き）

フィールド	説明
Rogue Detection Transient Interval (Enter 0 to Disable)	最初に不正がスキャンされた後、AP が継続的に不正をスキャンする必要のある間隔を入力します。一時的な間隔を入力することで、AP が不正をスキャンする間隔を制御できます。AP は、一時的な間隔の値に基づいて、不正をフィルタできます。有効な範囲は 120 ～ 1800 秒で、デフォルト値は 0 です。この機能は、監視モードの AP のみに適用されます。
Validate Rogue Clients against AAA	不正クライアントの AAA 検証を有効にする場合にオンにします。
Detect and Report Adhoc Networks	アドホック ネットワーキングに参加している不正クライアントの検出とレポートを有効にする場合にオンにします。
Rogue on Wire	有線ネットワークで検出された不正を自動的に封じ込めます。
Using our SSID	ネットワークの SSID をアドバタイズしている不正を自動的に封じ込めます。このパラメータをオフにしておくと、該当する不正が検出されても警告が生成されるだけです。
Valid Client on Rogue AP	信頼できるクライアントが関連付けられた不正アクセス ポイントを自動的に封じ込めます。このパラメータをオフにしておくと、該当する不正が検出されても警告が生成されるだけです。

[Controller] > [Security] > [Access Control Lists]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [Security] > [Access Control Lists] にある [Template Detail] の各フィールドについて説明します。

表 2-57　[Controller] > [Security] > [Access Control Lists]

フィールド	説明
ACL Type	IPv6 は、コントローラ バージョン 7.2.x からサポートされます。

関連項目

- 再利用可能なグループ化された IP アドレスを作成するには、[Controller] > [System] (2-60 ページ) を参照してください。
- 新しいプロトコル グループを作成するには、[Controller] > [Security] > [Protocol Groups] (2-59 ページ) を参照してください。

[Controller] > [Security] > [CPU Access Control List]

注　IPv6 での CPU ACL 設定は、このリリースではサポートされません。これは、仮想インターフェイスを除き、インターフェイスのコントローラのすべての IP アドレスが IPv4 を使用するためです。

「Creating a FlexConnect Access Control List Template（FlexConnect アクセス コントロール リスト テンプレートの作成）」（*『Cisco Prime Infrastructure 3.0 User Guide』*を参照）で確立した既存の ACL を使用して、中央処理装置（CPU）とネットワーク プロセッサ ユニット（NPU）間のトラフィック制御を設定します。

[Controller] > [Security] > [File Encryption]

このページでは、ファイル暗号化テンプレートの追加、または既存のファイル暗号化テンプレートの変更が可能です。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [Security] > [File Encryption] にある [Template Detail] の各フィールドについて説明します。

表 2-58　[Controller] > [Security] > [File Encryption]

フィールド	説明
Encryption Key Confirm Encryption Key	ちょうど 16 個の ASCII 文字から成る暗号キー テキスト文字列を入力します。

[Controller] > [Security] > [IP Groups]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [Security] > [IP Groups] にある [Template Detail] の各フィールドについて説明します。

関連項目

IPv6 グループを作成するには、[Controller] > [Security] > [IPv6 Groups]（2-58 ページ）を参照してください。

表 2-59　[Controller] > [Security] > [IP Groups]

フィールド	説明
IP Address	IPv4 アドレス形式を入力します。
NetmaskNotation	ネットマスクを入力すると、IP アドレス プロパティの CIDR 表記ではなく、ドット区切り 10 進数表記でサブネット マスクを設定できます。範囲内の IP アドレスを持つマシンだけにインターネット サービスへのアクセスを許可するために定義された IP アドレスの範囲。
CIDR Notation	クラスレス ドメイン間ルーティング（CIDR）表記は、複数の連続ブロックでのクラス C の IP アドレス割り当てを許可するプロトコルです。この表記を使用して、1 つのクライアント オブジェクトを設定するだけで、サブネット範囲に存在する大量のクライアントを追加できます。
List of IP Addresses/Netmasks	IP アドレス グループがすべて一覧表示されます。IP アドレス グループ 1 つで最高 128 の IP アドレスとネットマスクの組み合わせを格納できます。新しい IP アドレス グループを定義するには、[Add] を選択します。既存の IP アドレス グループを表示または変更するには、IP アドレス グループの URL をクリックします。[IP address group] ページが開きます。 **注**　IP アドレスが「any」の場合用に、「*any*」グループが定義されています。 [Move Up] ボタンおよび [Move Down] ボタンを使用して、リスト項目の順序を変更します。[Delete] ボタンを使用すると、IP アドレスまたはネットマスクを削除できます。

[Controller] > [Security] > [IPv6 Groups]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [Security] > [IPv6 Groups] にある [Template Detail] の各フィールドについて説明します。

関連項目

IPv4 グループを作成するには、[Controller] > [System]（2-60 ページ）を参照してください。

表 2-60　[Controller] > [Security] > [IPv6 Groups]

フィールド	説明
IP Address	IPv6 アドレス形式を入力します。
Prefix Length	IPv6 アドレスのプレフィクス(0 ～ 128)。
List of IP Addresses/Netmasks	IP アドレス グループがすべて一覧表示されます。IP アドレス グループ 1 つで最高 128 の IP アドレスとネットマスクの組み合わせを格納できます。新しい IP アドレス グループを定義するには、[Add] を選択します。既存の IP アドレス グループを表示または変更するには、IP アドレス グループの URL をクリックします。[IP address group] ページが開きます。 **注**　IP アドレスが「any」の場合用に、「*any*」グループが定義されています。 [Move Up] ボタンおよび [Move Down] ボタンを使用して、リスト項目の順序を変更します。[Delete] ボタンを使用すると、IP アドレスまたはネットマスクを削除できます。

[Controller] > [Security] > [Protocol Groups]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [Security] > [Protocol Groups] にある [Template Detail] の各フィールドについて説明します。

表 2-61　[Controller] > [Security] > [Protocol Groups]

フィールド	説明
Rule Name	既存のルールの場合はルール名が表示され、新しいルールの場合は名前を入力できます。ルールを定義するために ACL は必要ありません。パケットがルールのすべてのフィールドに一致すると、このルールに対する動作が実行されます。
Protocol	ドロップダウン リストからプロトコルを選択します。 • [Any]:すべてのプロトコル • [TCP]:トランスミッション コントロール プロトコル • [UDP]:ユーザ データグラム プロトコル • [ICMP]:インターネット制御メッセージ プロトコル • [ESP]:IP Encapsulating Security Payload • [AH]:認証ヘッダー • [GRE]:Generic Routing Encapsulation • [IP]:インターネット プロトコル • [Eth Over IP]:Ethernet over Internet Protocol • [Other Port OSPF]:Open Shortest Path First • [Other]:その他の任意の IANA プロトコル(http://www.iana.org/) 一部のプロトコル(TCP または UDP など)を選択すると、追加の送信元ポートおよび宛先ポート GUI エレメントが表示されます。
Source Port	送信元ポートを入力します。[Any]、[HTTP]、[HTTPS]、[Telnet]、[RADIUS]、[DHCP Server]、[DHCP Client]、[DNS]、[L2TP]、[PPTP control]、[FTP control]、[SMTP]、[SNMP]、[LDAP]、[Kerberos]、[NetBIOS NS]、[NetBIOS DS]、[NetBIOS SS]、[MS Dir Server]、[Other]、[Port Range] を指定できます。

表 2-61　[Controller] > [Security] > [Protocol Groups]（続き）

フィールド	説明
Dest Port	宛先ポートを入力します。[TCP] または [UDP] が選択されている場合、[Any]、[HTTP]、[HTTPS]、[Telnet]、[RADIUS]、[DHCP Server]、[DHCP Client]、[DNS]、[L2TP]、[PPTP control]、[FTP control]、[SMTP]、[SNMP]、[LDAP]、[Kerberos]、[NetBIOS NS]、[NetBIOS DS]、[NetBIOS SS]、[MS Dir Server]、[Other]、[Port Range] を指定できます。
DSCP (Differentiated Services Code Point)	ドロップダウン リストから [Any] または [Specific] を選択します。[Specific] を選択した場合は DSCP（0 ～ 255）を入力します。DSCP は、インターネットでのサービスの質を定義するために使用できるパケット ヘッダー コードです。

[Controller] > [System]

次に、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [System] にあるページの各フィールドについて説明します。

- [Controller] > [System] > [AP Username Password]（2-60 ページ）
- [Controller] > [System] > [DHCP]（2-61 ページ）
- [Controller] > [System] > [Dynamic Interface]（2-61 ページ）
- [Controller] > [System] > [General]（2-63 ページ）
- [Controller] > [System] > [Global CDP Configuration]（2-67 ページ）
- [Controller] > [System] > [QoS Profiles]（2-67 ページ）
- [Controller] > [System] > [SNMP Community]（2-68 ページ）
- [Controller] > [System] > [Traffic Stream Metrics QoS]（2-68 ページ）
- [Controller] > [System] > [User Roles]（2-69 ページ）
- [Controller] > [WLANs] > [WLAN Configuration]（2-69 ページ）

[Controller] > [System] > [AP 802.1X Supplicant Credentials]

このオプションを使用して、Lightweight アクセス ポイントとスイッチ間の 802.1X 認証を設定します。アクセス ポイントは 802.1X サプリカントとして動作し、EAP-FAST と匿名 PAC プロビジョニングを使用してスイッチにより認証されます。すべてのアクセス ポイントがコントローラ接続時に継承するグローバル認証を設定できます。これには、コントローラに現在接続されているすべてのアクセス ポイント、および今後接続されるすべてのアクセス ポイントが含まれます。

このテンプレートの作成に関する基本情報については、*『Cisco Prime Infrastructure 3.0 User Guide』*の「Creating Feature-Level Configuration Templates（機能レベルの設定テンプレートの作成）」を参照してください。

[Controller] > [System] > [AP Username Password]

このオプションを使用して、アクセス ポイントのユーザ名およびパスワードを設定するテンプレートを作成または変更します。すべてのアクセス ポイントは、コントローラに接続されるときにパスワードを継承します。これらのクレデンシャルは、コンソールまたは Telnet/SSH を介してアクセス ポイントにログインするときに使用されます。

[AP Username Password] ページでは、すべてのアクセス ポイントがコントローラに接続する際に継承する、グローバル パスワードを設定できます。また、アクセス ポイントを追加するときに、このグローバル ユーザ名およびパスワードを受け入れるか、アクセス ポイント単位で上書きするかを選択できます。

さらにコントローラ ソフトウェア リリース 5.0 では、アクセス ポイントをコントローラに接続すると、そのアクセス ポイントのコンソール ポート セキュリティが有効になり、アクセス ポイント コンソール ポートへログインするたびにユーザ名とパスワードの入力を要求されます。ログインした時点では非特権モードのため、特権モードを使用するには、有効化パスワードを入力する必要があります。

このテンプレートの作成に関する基本情報については、『*Cisco Prime Infrastructure 3.0 User Guide*』の「Creating Feature-Level Configuration Templates（機能レベルの設定テンプレートの作成）」を参照してください。

[Controller] > [System] > [DHCP]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [System] > [DHCP] にある [Template Detail] の各フィールドについて説明します。

表 2-62　[Controller] > [System] > [DHCP]

フィールド	説明
DHCP Option 82 Remote Id field format	このフィールドで、DHCP を使用してネットワーク アドレスを割り当てる場合のセキュリティを強化します。具体的には、コントローラが DHCP リレー エージェントとして動作して、信頼できないソースからの DHCP クライアント要求を阻止できるようにします。DHCP 要求にオプション 82 情報を追加してから DHCP サーバに転送するように、コントローラを設定することができます。
DHCP Proxy	WLAN ベースではなく、グローバルに DHCP プロキシを有効にするには、[DHCP Proxy] チェックボックスをオンにします。 DHCP プロキシがコントローラ上で有効になっている場合は、コントローラによってクライアントから設定済みサーバへ DHCP 要求がユニキャストされます。少なくとも 1 つの DHCP サーバが、WLAN にアソシエートされたインターフェイスか WLAN 自体で設定されている必要があります。
DHCP Timeout	（バージョン 7.0.114.74 以降のコントローラの場合）DHCP タイムアウトを秒単位で入力します。

[Controller] > [System] > [Dynamic Interface]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [System] > [Dynamic Interface] にある [Template Detail] の各フィールドについて説明します。

表 2-63　[Controller] > [System] > [Dynamic Interface]

フィールド	説明
Guest LAN	インターフェイスを有線としてマークする場合にオンにします。
Quarantine	VLAN の検疫を有効または無効にします。チェックボックスをオンにすると有効になります。
Netmask	インターフェイスのネットマスク アドレスを入力します。

表 2-63　[Controller] > [System] > [Dynamic Interface]（続き）

フィールド	説明
LAG Mode	LAG モードを有効にするには、このチェックボックスをオンにします。このインターフェイスで LAG モードを選択した場合は、LAG 対応コントローラにのみ設定が適用されます。
Primary Port Number	インターフェイスに現在使用されているポートを入力します。
Secondary Port Number	セカンダリ ポートを入力します。セカンダリ ポートは、プライマリ ポートがダウンしているときにインターフェイスにより使用されます。プライマリ ポートが再アクティブ化されると、Cisco 4400 シリーズ Wireless LAN Controller は、インターフェイスをプライマリ ポートに転送されます。 プライマリおよびセカンダリのポート番号は、Cisco 4400 Series Wireless LAN コントローラにのみ存在します。
AP Management	アクセス ポイントの管理を有効にするには、このチェックボックスをオンにします。
Primary DHCP Server	プライマリ DHCP サーバの IP アドレスを入力します。
WINS Server	セカンダリ DHCP サーバの IP アドレスを入力します。
ACL Name	定義済みの名前のリストから名前を選択します。 [Add Interface Format Type] グループ ボックスの [Add Format Type] ドロップダウンリストから、[Device Info] または [File] のいずれかを選択します。[Device Info] を選択する場合、各コントローラのデバイス固有フィールドを設定する必要があります。[File] を選択する場合、CSV ファイルで指定されているすべての管理対象コントローラの CSV デバイス固有フィールド（[Interface Name]、[VLAN Identifier]、[Quarantine VLAN Identifier]、[IP Address]、[Gateway]）を設定する必要があります（次の表を参照）。

サンプル CSV ファイルを次に示します。

表 2-64　サンプル CSV ファイル

ip_address	interface_name	vlan_id	quarantine_vlan_id	interface_ip_address	gateway
209.165.200.224	dyn-1	1	2	209.165.200.228	209.165.200.229
209.165.200.225	interface-1	4	2	209.165.200.230	209.165.200.231
209.165.200.226	interface-2	5	3	209.165.200.232	209.165.200.233
209.165.200.227	dyna-2	2	3	209.165.200.234	209.165.200.235

CSV ファイルの最初の行は、含まれている列の説明に使用されます。CSV ファイルには、次のフィールドを含めることができます。

- ip_address
- interface_name
- vlan_id
- quarantine_vlan_id
- interface_ip_address
- gateway

[Apply to Controllers] を選択した場合、[Apply To] ページに進みます。このページで、各コントローラのデバイス固有フィールドを設定できます。

[Add] および [Remove] オプションを使用して、各コントローラのデバイス固有フィールドを設定します。[Edit] をクリックすると、現在のパラメータ入力を示すダイアログボックスが表示されます。

ダイアログボックスで必要な変更を行い、[OK] をクリックします。

注　インターフェイス フィールドを変更する場合、WLAN が一時的に無効になるため、一部のクライアントとの接続が切断されることがあります。インターフェイス フィールドの変更は、コントローラに正常に適用された後で保存されます。

注　ここでインターフェイスを削除すると、インターフェイスは、コントローラではなく、テンプレートからのみ削除されます。

[Controller] > [System] > [General]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [System] > [General - System] にある [Template Detail] の各フィールドについて説明します。

表 2-65　[Controller] > [System] > [General - System Template]

フィールド	説明
802.3x Flow Control Mode	フロー制御モードを有効または無効にします。
802.3 Bridging	802.3 ブリッジングを有効または無効にします。Cisco 5500 シリーズおよび Cisco 2106 シリーズのコントローラについては、この 802.3 ブリッジング オプションは使用できません。
Web Radius Authentication	必要な Web RADIUS 認証を選択します。ユーザ資格情報の交換時に、コントローラとクライアント間の認証用に、PAP、CHAP、または MD5-CHAP の使用を選択できます。
AP Primary Discovery Timeout	AP Primary Discovery タイムアウトの秒数を指定します。デフォルトは 120 秒で、有効な範囲は 30 ～ 3600 秒です。
Back-up Primary Controller IP Address	バックアップのプライマリ コントローラおよびセカンダリ コントローラの詳細を指定します。
Back-up Primary Controller Name	
Back-up Secondary Controller IP Address	
Back-up Secondary Controller Name	
CAPWAP Transport Mode	レイヤ 2 またはレイヤ 3 転送モードを指定します。レイヤ 3 に設定した場合、Lightweight アクセス ポイントは IP アドレスを使用してアクセス ポイントと通信します。これらの IP アドレスは必須の DHCP サーバから収集します。レイヤ 2 に設定した場合、Lightweight アクセス ポイントは専用コードを使用してアクセス ポイントと通信します。 バージョン 5.2 までのコントローラでは LWAPP が使用され、新しいコントローラ バージョンでは CAPWAP が使用されます。

表 2-65　[Controller] > [System] > [General - System Template]（続き）

フィールド	説明
Broadcast Forwarding	ブロードキャスト転送を有効または無効にします。デフォルトでは無効になっています。
LAG Mode	[LAG Mode] ドロップダウン リストから [Enable] または [Disable] を選択します。リンク集約によって、物理ポートをすべてグループ化してリンク集約グループ（LAG）を作成し、コントローラ上のポートを構成するために必要な IP アドレスの数を削減できます。 LAG がコントローラで有効にされている場合、インターフェイス データベース内での設定の矛盾を避けるため、作成したダイナミック インターフェイスが削除されます。LAG 設定に変更を加えると、変更を有効にするためにコントローラをリブートする必要があります。 インターフェイスは Dynamic AP Manager フラグを設定した状態では作成できません。また、コントローラ上では複数の LAG を作成できません。
Peer to Peer Blocking Mode	ピアツーピア ブロック モードを有効にするか無効にするかを選択します。[Disable] を選択すると、同じサブネットのクライアントはすべてこのコントローラを使用して通信します。[Enable] を選択すると、同じサブネットのクライアントはすべて上位レベルのルータを使用して通信します。
Over-the-Air Provisioning AP Mode	[Over Air AP Provision Mode] ドロップダウン リストから、[enable] または [disable] を選択します。
AP Fallback AP Failover Priority	[AP Fallback] ドロップダウン リストで、[enable] または [disable] を選択します。フォールバックを有効にすると、プライマリ コントローラの接続を切断されたアクセス ポイントがプライマリ コントローラの復帰と同時に自動的にサービスに戻ります。 コントローラに障害が発生した場合、アクセス ポイントに設定されたバックアップ コントローラがすぐに多くの検出と接続要求を受信します。これにより、コントローラは飽和ポイントに達し、いくつかのアクセス ポイントを拒否する可能性があります。優先順位をアクセス ポイントに割り当てることによって、拒否されるアクセス ポイントを制御します。フェールオーバー時にバックアップ コントローラが飽和している状況では、優先度の低いアクセス ポイントの接続を切断すると、優先度の高いアクセス ポイントがバックアップ コントローラに接続できるようになります。この機能を有効にする場合、[AP Failover Priority] ドロップダウン リストから [enable] を選択します。
Apple Talk Bridging	AppleTalk ブリッジングを有効にするか無効にするかを選択します。 この AppleTalk ブリッジング オプションは、Cisco 5500 シリーズ コントローラでは使用できません。

表 2-65　[Controller] > [System] > [General - System Template]（続き）

フィールド	説明
Fast SSID Change	[Fast SSID Change] オプションを有効にするか無効にするかを選択します。このオプションを有効にすると、クライアントは SSID 間で接続をほとんど中断せずにコントローラに瞬時に接続します。通常、各クライアントは SSID に特定された特定の WLAN に接続します。クライアントが接続したアクセス ポイントの範囲外に移動した場合、クライアントは別のアクセス ポイントを使用してコントローラに再接続する必要があります。この通常のプロセスは、DHCP サーバが IP アドレスをクライアントに割り当てる必要があるため、少し時間がかかります。 マスター コントローラは、通常、展開されたネットワークで使用されないため、マスター コントローラの設定は、リブートまたはオペレーティング システム コードのアップグレード時に自動的に無効になります。コントローラをマスター コントローラとして [Master Controller Mode] ドロップダウン リストから有効にする場合もあります。
Master Controller Mode	無線クライアントからコントローラ管理インターフェイスへのアクセスを有効にするか無効にするかを選択します。IPsec 動作により、無線による管理は WPA または静的 WEP 全体にログインしているオペレータだけが実行できます。
Wireless Management	ワイヤレス管理は、IPsec WLAN を経由してログインしようとしているクライアントは実行できません。
Symmetric Tunneling Mode	シンメトリック トンネリング モードを有効にするか無効にするかを選択します。シンメトリック モビリティ トンネリングを使用すると、コントローラでは 1 つのアクセス ポイントから無線 LAN 内の別のアクセス ポイントへローミングするクライアントに対して、サブネット間のモビリティが提供されます。有線ネットワーク上のクライアント トラフィックは、外部コントローラによって直接ルーティングされます。ルータでリバース パス転送（RPF）が有効になっている場合、受信パケットで追加確認が実行され、通信はブロックされます。RPF が有効になっている場合でも、シンメトリック モビリティ トンネリングによって、アンカーとして指定されたコントローラにクライアント トラフィックが到達できるようになります。 モビリティ グループのすべてのコントローラは、同一のシンメトリック トンネリング モードを備えている必要があります。 シンメトリック トンネリングを有効にするには、リブートする必要があります。
ACL Counters	[ACL Counters] ドロップダウン リストを使用して、ACL カウンタを有効または無効にします。各コントローラの ACL ルールごとの値を表示できます。
Default Mobility Domain Name	[Default Mobility Domain Name] テキスト ボックスにオペレータが定義した RF モビリティ グループ名を入力します。
Mobility Anchor Group Keep Alive Interval	クライアントが別のアクセス ポイントへの接続を試みるまでの遅延時間を指定します。このゲスト トンネリングの N+1 冗長機能を使用すると、コントローラのエラー後にクライアントが別のアクセス ポイントに接続するためにかかる時間が短縮されます。エラーがすばやく特定され、クライアントが問題発生のコントローラから移動し、別のコントローラに接続されるためです。 マウス カーソルをフィールドの上に移動すると、値の有効な範囲が表示されます。

表 2-65　[Controller] > [System] > [General - System Template]（続き）

フィールド	説明
Mobility Anchor Group Keep Alive Retries	クライアントが到達不能であると宣言するまで、アンカーするクエリの数を指定します。
RF Network Name	8 ～ 19 文字で RF ネットワーク グループ名を入力します。無線リソース管理（RRM）ネイバー パケットは RF ネットワーク グループ内のアクセス ポイントに分散されます。Cisco アクセス ポイントは、この RF ネットワーク名で送信された RRM ネイバー パケットだけを受け入れます。別の RF ネットワーク名で送信された RRM ネイバー パケットはドロップされます。
User Idle Timeout	アイドル クライアントのタイムアウトを指定します。デフォルトは 300 秒です。タイムアウトを過ぎると、クライアントは認証を失い、アクセス ポイントから一時的に関連付けを解除し、再度関連付けて、再認証を行います。 アドレス解決プロトコルのタイムアウトを秒単位で指定します。デフォルトは 300 秒です。
ARP Timeout	タイムアウトを秒単位で指定します。
Global TCP Adjust MSS	[Global TCP Adjust MSS] チェックボックスをオンにすると、クライアントから送信される TCP パケットが、TCP SYN/TCP ACK パケットおよび MSS 値に対してチェックされ、アップストリームおよびダウンストリーム側の設定値にリセットされます。
Disable local access	このチェックボックスをオンにすると、AP はローカル SSID をブロードキャストしなくなったり、すべてのイーサーネット ポートへのアクセスを許可しなくなります。
Out of Box	無線とともに、設定済みの AP グループの両方に設定済みの RF プロファイルを作成するには、このチェックボックスをオンにします。
Web Auth Proxy Redirect Mode	手動プロキシ設定がクライアントのブラウザで設定されている場合、[Web Auth Proxy Redirect Mode] の [enable] または [disable] を選択します。このクライアントから送信されるすべての Web トラフィックは、ブラウザで設定されている PROXY IP および PORT に送信されます。
Web Auth Proxy Redirect Port	Enter the Web Auth Proxy Redirect Port.デフォルトのポートは、8080 および 3128 です。範囲は 0 ～ 65535 です。
AP Retransmit Count AP Retransmit Interval	[AP Retransmit Count] および [AP Retransmit Interval] に値を入力します。[AP Retransmit Count] のデフォルト値は 5 で、範囲は 3 ～ 8 です。[AP Retransmit Interval] のデフォルト値は 3 です。範囲は 2 ～ 5 です。

[Controller] > [System] > [Global CDP Configuration]

Cisco Discovery Protocol（CDP）は、すべてのシスコ製ネットワーク機器で実行されるデバイス検出プロトコルです。各デバイスはマルチキャスト アドレスに識別メッセージを送信し、他のデバイスから送信されたメッセージをモニタします。CDP は、デフォルトでイーサネットと、ブリッジの無線ポートで有効です。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [System] > [Global CDP Configuration] にある [Template Detail] の各フィールドについて説明します。

表 2-66　[Controller] > [System] > [Global CDP Configuration Template]

フィールド	説明
CDP on controller	コントローラで CDP を有効にするか、無効にするかを選択します。この設定は、WiSM2 コントローラには適用できません。
Global CDP on APs	アクセス ポイントで CDP を有効にするか、無効にするかを選択します。
Refresh-time Interval	CDP メッセージが生成される時間を秒単位で入力します。デフォルトは 60 です。
Holdtime	CDP ネイバー エントリの期限が切れるまでの時間を秒単位で入力します。デフォルトは 180 です。
CDP Advertisement Version	使用する CDP プロトコルのバージョンを入力します。デフォルトは v1 です。
Ethernet Interface Slot	CDP を有効にするイーサネット インターフェイスのスロットを選択します。[CDP for Ethernet Interfaces] フィールドは、バージョン 7.0.110.2 以降のコントローラでサポートされています。
Radio Interface Slot	CDP を有効にする無線インターフェイスのスロットを選択します。[CDP for Radio Interfaces] フィールドは、バージョン 7.0.110.2 以降のコントローラでサポートされています。

[Controller] > [System] > [QoS Profiles]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [System] > [QoS Profiles] にある [Template Detail] の各フィールドについて説明します。

表 2-67　[Controller] > [System] > [QoS Profiles Template]

フィールド	説明
Per-User Bandwidth Contracts	**注**　すべてに 0 または Off のデフォルトがあります。
Average Data Rate	UDP 以外のトラフィックの平均データ レート。
Global CDP on APs	UDP 以外のトラフィックのピーク データ レート。
Average Real-time Rate	UDP トラフィックの平均データ レート。
Burst Real-time Rate	UDP トラフィックのピーク データ レート。
Over-the-Air QoS	**注**　無線 QoS 設定は、コントローラ バージョン 7.0 以前のバージョンに適用できます。
Maximum QoS RF Usage per AP	クライアントに利用可能な最大エア帯域幅。デフォルトは 100 % です。
QoS Queue Depth	クライアントのクラスのキュー深度。これより大きな値のパケットは、アクセス ポイントでドロップされます。

表 2-67　[Controller] > [System] > [QoS Profiles Template]（続き）

フィールド	説明
Wired QoS Protocol	
Wired QoS Protocol	802.1P プライオリティ タグをアクティブにするには 802.1P を選択し、802.1P プライオリティ フラグを非アクティブにするには [None] を選択します。
802.1P Tag	有線接続の 802.1P プライオリティ タグを 0 ～ 7 の範囲で選択します。このタグは、トラフィックおよび CAPWAP パケットに使用されます。

[Controller] > [System] > [SNMP Community]

このオプションを使用して、コントローラでの SNMP コミュニティの設定用のテンプレートを作成または変更します。SNMP コミュニティのみが SNMPv1 および v2c に適用されます。SNMPv3 はユーザ名とパスワードを使用します。

このテンプレートの作成に関する基本情報については、*『Cisco Prime Infrastructure 3.0 User Guide』*の「Creating Feature-Level Configuration Templates（機能レベルの設定テンプレートの作成）」を参照してください。

SNMP コミュニティ情報を入力する際にアクセス モード オプションを [Read Only] に設定した場合は、このテンプレートを設定した後は *Prime Infrastructure にはコントローラへの読み取りアクセスのみが備わります。*

[Controller] > [System] > [Traffic Stream Metrics QoS]

トラフィック ストリーム メトリックは、無線 LAN での VoIP に関する一連の統計で、無線 LAN の QoS について報告します。これらの統計は、VoIP システムにより提供されるエンドツーエンドの統計とは異なります。エンドツーエンドの統計は、コール パスからなるすべてのリンクをカバーする、パケット損失および遅延に関する情報を提供します。しかし、トラフィック ストリーム メトリックは、コールの WLAN セグメントだけの統計です。このためシステム管理者は、音声の問題が WLAN によるものであるのか、コールに関与するその他のネットワーク要素によるものであるのかを、迅速に判断できます。どのアクセス ポイントの QoS が低下しているかを監視することにより、システム管理者は問題の発生している物理領域を迅速に特定できます。無線のカバレッジ不足または過度の干渉が根本的な問題である場合は、これが重要となります。

音声コールの音声品質に影響を与える可能性のある 4 つの QoS の値（パケット遅延、パケット ジッタ、パケット損失、ローミング時間）がモニタされます。このプロセスには、すべての無線 LAN コンポーネントが関与しています。アクセス ポイントおよびクライアントでメトリックを測定し、アクセスポイントで計測結果を収集してこれらをコントローラに送信します。アクセス ポイントでは、90 秒ごとにコントローラのトラフィック ストリーム メトリック情報を更新し、一度に 10 分間分のデータが格納されます。Prime Infrastructure はコントローラにメトリックを問い合わせ、[Traffic Stream Metrics QoS Status] にこれらを表示します。これらのメトリックは閾値と比較され、ステータス レベルが決定されます。統計のいずれかのステータス レベルが可（黄色）または低下（赤）と表示された場合には、管理者は無線 LAN の QoS を調査します。

アクセス ポイントで測定値を収集するには、トラフィック ストリーム メトリックがコントローラで有効であることが必要です。

[Traffic Stream Metrics QoS Controller Configuration] ページにいくつかの QoS 値が示されます。管理者は、音声およびビデオの次の品質をモニタできます。

- Upstream delay
- Upstream packet loss rate

- Roaming time
- Downstream packet loss rate
- Downstream delay

パケット損失率（PLR）は音声の明瞭さに影響を与えます。パケット遅延は、明瞭さと接続におけるやり取りの品質の両方に影響を与える可能性があります。過度のローミング時間は音声に望ましくないギャップが生じます。

測定レベルは 3 つあります。

- Normal：正常な QoS（緑）
- Fair：一応は満足できる QoS（黄色）
- Degraded：低下した QoS（赤）

緑、黄色、および赤のアラーム レベルを設定する際、システム管理者は何らかの判断を採る必要があります。考慮すべきファクタは次のとおりです。

- PLR に影響を与える可能性のある干渉および無線のカバレッジを含む環境ファクタ。
- モバイル デバイスでの音声品質に対するエンド ユーザの期待およびシステム管理者の要求（音声品質が低いほど高い PLR が可能）。
- 電話により使用されるコーデックの種類が異なると、パケット損失の許容値は異なる。
- すべてのコールがモバイル間のコールとは限らず、そのため、中には無線 LAN に関する PLR 要件があまり厳しくないものがある。

[Controller] > [System] > [User Roles]

このオプションを使用して、ユーザ ロール設定用のテンプレートを作成または変更します。ユーザ ロールは、ネットワークが使用できる帯域幅の量を決定します。ゲスト ユーザに割り当てる帯域幅には、4 つの QoS レベル（プラチナ、ブロンズ、ゴールドおよびシルバー）を使用できます。ゲスト ユーザには、ロール（契約者、顧客、代理店、ベンダー、ビジター、その他）が事前に割り当てられます。また、それぞれの帯域幅は、管理者により設定されます。これらの役割は、新しいゲスト ユーザを追加するときに適用できます。

このテンプレートの作成に関する基本情報については、*『Cisco Prime Infrastructure 3.0 User Guide』*の「Creating Feature-Level Configuration Templates（機能レベルの設定テンプレートの作成）」を参照してください。

[Controller] > [WLANs] > [WLAN Configuration]

WLAN テンプレートを利用すると、複数のコントローラに適用するためのさまざまな WLAN プロファイルを定義できます。

注　同じ SSID の WLAN を複数設定できます。この機能によって、同じ無線 LAN 内で別のレイヤ 2 セキュリティ ポリシーを割り当てられます。WLAN 設定テンプレートを展開すると、インターフェイス/インターフェイス グループ、選択した RADIUS サーバ、LDAP サーバ、ACL 名とルール、および入力インターフェイスが [Template Deployment - Prepare and Schedule] ページに表示されます。

次の制限は、同じ SSID で複数の WLAN を設定する場合に適用されます。

- 同じ SSID の WLAN は、クライアントがビーコンおよびプローブ内のアドバタイズされた情報に基づいて WLAN を選択できるように、一意のレイヤ 2 セキュリティ ポリシーを持っている必要があります。利用できるレイヤ 2 セキュリティ ポリシーは次のとおりです。

  - なし（オープン WLAN）
  - 静的 WEP または 802.1
  - CKIP
  - WPA/WPA2
- SSID を共有する WLAN 上で Broadcast SSID を有効にする必要があります。これによって、アクセス ポイントがこれらの WLAN のプローブ応答を生成できます。
- FlexConnect アクセス ポイントは、複数の SSID をサポートしません。

次に、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [WLANs] > [WLAN Configuration] の各フィールドについて説明します。

- [Controller] > [WLANs] > [WLAN Configuration] > [General]（2-70 ページ）
- [Controller] > [WLANs] > [WLAN Configuration] > [Security]（2-71 ページ）
- [Controller] > [WLANs] > [WLAN Configuration] > [QoS]（2-76 ページ）
- [Controller] > [WLANs] > [WLAN Configuration] > [Advanced]（2-77 ページ）
- [Controller] > [WLANs] > [WLAN Configuration] > [HotSpot]（2-82 ページ）

[Controller] > [WLANs] > [WLAN Configuration] > [General]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [WLANs] > [WLAN Configuration] > [General] にある [Template Detail] の各フィールドについて説明します。

表 2-68　[Controller] > [WLANs] > [WLAN Configuration] > [General]

フィールド	説明
Wired LAN	このチェックボックスをオンにし、この WLAN が有線 LAN かどうかを示します。 **注**　ゲスト アクセスに指定および設定したイーサネット接続から有線ゲスト アクセスをゲスト ユーザに設定するかどうかを指定します。有線ゲスト アクセス ポートは、ゲストのオフィスまたは会議室の特定のポートで使用できます。Lobby Ambassador ポータルを使用してアカウントがネットワークに追加されます。（出力インターフェイスまたは入力インターフェイスの設定は、有線 LAN のみで使用できます。） [Type] ドロップダウン リストを使用して、有線 LAN のタイプを選択します。 • [Guest LAN]：この有線 LAN がゲスト LAN であることを示します。[Guest LAN] オプションを選択した場合、任意のゲスト LAN に割り当てられていない出力kインターフェイスを選択する必要があります。 • [Remote LAN]：有線 LAN がリモート LAN であることを示します。
Profile Name	WLAN またはゲスト LAN を示す [Profile Name] テキスト ボックスに名前を入力します。入力する名前には、スペースを使用しないでください。
SSID	WLAN SSID の名前を入力します。SSID は、ゲスト LAN には必要ありません。 同じ SSID の WLAN は、クライアントがビーコンおよびプローブ内のアドバタイズされた情報に基づいて WLAN を選択できるように、一意のレイヤ 2 セキュリティ ポリシーを持っている必要があります。
Status	[Status] フィールドで [Enable] チェックボックスをオンにします。

表 2-68　[Controller] > [WLANs] > [WLAN Configuration] > [General]（続き）

フィールド	説明
Configure Wlan Id	WLAN に識別子を指定するには、このチェックボックスをオンにします。 WLAN 識別子（整数）を入力するには、[Wlan Id] テキスト ボックスを使用します。
Security Policies	[Security] タブで行った変更は、テンプレートを保存した後に表示されます。
Radio Policy	[All]（802.11a/b/g/n）、[802.11a only]、[802.11g only]、[802.11b/g only]、または [802.11a/g only] に適用する WLAN ポリシーを設定します。
Interface/Interface Group	[Controller] > [Interfaces] モジュールで作成したインターフェイスの利用可能な名前を選択します。
Multicast VLAN	[Enable] チェックボックスをオンにし、マルチキャスト VLAN 機能を有効にします。 [Multicast VLAN Interface] ドロップダウン リストから、適切なインターフェイス名を選択します。このリストは、マルチキャスト VLAN 機能を有効にすると自動的に読み込まれます。
Broadcast SSID	この WLAN について SSID ブロードキャストをアクティブ化する場合にオンにします。

[Controller] > [WLANs] > [WLAN Configuration] > [Security]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [WLANs] > [WLAN Configuration] > [Security] にある [Template Detail] の各フィールドについて説明します。

表 2-69　[Controller] > [WLANs] > [WLAN Configuration] > [Security]

フィールド	説明
レイヤ 2	
None	レイヤ 2 の選択はありません。 • [FT Enable]：アクセス ポイント間の高速移行（FT）を有効にする場合は、このチェックボックスをオンにします。 **注**　高速移行は FlexConnect モードではサポートされません。 [Over the DS]：分散システム（DS）での高速移行を有効にする場合は、このチェックボックスをオンにします。 [Reassociation Timeout]：高速移行の再関連付けがタイムアウトするまでの時間（秒単位）。デフォルトは 20 秒です。有効な範囲は 1 ～ 100 です。 [Over the DS] または [Reassociation Timeout] を有効にするには、高速移行を有効にする必要があります。
802.1X	WEP 802 1X データ暗号化タイプ。 • 40/64 ビット キー • 104 ビット キー • 152 ビット キー

表 2-69　[Controller] > [WLANs] > [WLAN Configuration] > [Security]（続き）

フィールド	説明
Static WEP	静的 WEP 暗号化フィールド: • [Key sizes]:設定なし、40/64、104 および 152 ビット キー サイズ。 • [Key Index]:1 ～ 4。 • [Encryption Key]:暗号キーは必須です。 • [Key Format]:ASCII または HEX。 • [Allowed Shared Key Authentication]:チェックボックスをオンにすると、共有キー認証が有効になります。 選択した形式に関係なく、セキュリティ上の理由で、ASCII のみが WLC（および Prime Infrastructure）に表示されます。そのため、自動プロビジョニング時にテンプレートを使用しても、別のコントローラの設定を複製できません。検出されたテンプレートが別のデバイスに適用される場合、テンプレートでもう一度キー形式を設定する必要があります。
Static WEP-802.1X	この設定により、静的 WEP と 802.1X の両方のポリシーを有効にします。このオプションを選択すると、静的 WEP と 802.1X のフィールドがページの下部に表示されます。 静的 WEP 暗号化フィールド: • [Key sizes]:設定なし、40/64、104 および 152 ビット キー サイズ。 • キー インデックス:1 ～ 4。 • [Encryption Key]:暗号キーを入力します。 • [Key Format]:ASCII または HEX。 • [Allowed Shared Key Authentication]:チェックボックスをオンにすると有効になります。 • 802.1 データ暗号化:40/64 ビット キー、104 ビット キー、152 ビット キー。
CKIP	Cisco Key Integrity Protocol（CKIP）。Cisco のアクセス ポイントは、ビーコンおよびプローブの応答パケットで CKIP のサポートをアドバタイズします。CKIP は、Aironet IE が WLAN で有効な場合にだけ設定できます。 **注**　CKIP は 10xx AP ではサポートされていません。 選択すると、これらの CKIP フィールドが表示されます。 • [Key size]:設定なし、40 または 104。 • [Key Index]:1 ～ 4。 • [Encryption Key]:暗号キーを指定します。 • [Key Format]:ASCII または HEX。 **注**　選択した形式に関係なく、セキュリティ上の理由で、ASCII のみが WLC（および Prime Infrastructure）に表示されます。そのため、自動プロビジョニング時にテンプレートを使用しても、別のコントローラの設定を複製できません。検出されたテンプレートが別のデバイスに適用される場合、テンプレートでもう一度キー形式を設定する必要があります。 [MMH Mode]:チェックボックスをオンにすると有効になります。 [Key Permutation]:チェックボックスをオンにすると有効になります。

表 2-69　[Controller] > [WLANs] > [WLAN Configuration] > [Security]（続き）

フィールド	説明
MAC Filtering	MAC アドレスでクライアントをフィルタリングする場合にオンにします。 **注**　MAC フィルタ リスト内で指定されていなくてもコントローラに接続できるのは、メッシュ アクセス ポイントだけです。 **注**　4.1.82.0 以前のリリースでは、メッシュ アクセス ポイントは MAC フィルタ リストで定義されていない限り、コントローラに接続しません。 新しく追加されたアクセス ポイントがコントローラに接続できるようにするには、MAC フィルタ リストを無効にします。MAC フィルタ リストを再度有効にする前に、新しいアクセス ポイントの MAC アドレスを入力する必要があります。
Authentication Key Management（認証キー管理）	目的の種類の認証キー管理を選択します。802.1X、CCKM または PSK を選択できます。 **注**　PSK を選択した場合は、共有キーと種類（ASCII または 16 進数）を入力する必要があります。 **注**　選択した形式に関係なく、セキュリティ上の理由で、ASCII のみが WLC（および Prime Infrastructure）に表示されます。そのため、自動プロビジョニング時にテンプレートを使用しても、別のコントローラの設定を複製できません。検出されたテンプレートが別のデバイスに適用される場合、テンプレートでもう一度キー形式を設定する必要があります。
レイヤ 3	
Layer 3 Security	[None] または [VPN Pass Through] のいずれかを選択します。 **注**　VPN パススルー オプションは、2106 シリーズおよび 5500 シリーズのコントローラでは使用できません。

表 2-69　[Controller] > [WLANs] > [WLAN Configuration] > [Security]（続き）

フィールド	説明
Web Policy	デフォルトのスタティック WEP(Web 認証)を変更するか、または特定の Web 認証(ログイン、ログアウト、ログイン失敗)ページとサーバ ソースを割り当てることができます。 1. スタティック WEP をパスルーに変更するには、[Web Policy] チェックボックスをオンにして、ドロップダウン リストから [Passthrough] オプションを選択します。これでユーザは、ユーザ名やパスワードを入力しなくてもネットワークにアクセスできます。 [Email Input] チェックボックスが表示されます。ユーザがネットワークに接続しようとしたとき、電子メール アドレスの入力を求める場合は、このチェックボックスをオンにします。 2. [WebAuth on MAC Filter Failure] オプションをオンにすると、クライアントが MAC フィルタで失敗すると、自動的に webAuth に切り替えられます。 注　[WebAuth on Mac Filter Failure] オプションは、[Layer 2 Mac Filtering] オプションが有効な場合だけ機能します。 3. カスタムな Web 認証ページを指定するには、[Global WebAuth Configuration] の [Enable] チェックボックスをオフにします。 [Web Auth Type] ドロップダウン リストが表示されたら、次のいずれかのオプションを選択して、無線ゲスト ユーザ用の Web ログイン ページを定義します。 [Default Internal]:コントローラのデフォルト Web ログイン ページを表示します。これはデフォルト値です。 [Customized Web Auth]:カスタム Web ログイン ページ、ログイン失敗ページ、およびログアウト ページを表示します。[Customized] オプションを選択した場合は、ログイン ページ、ログイン失敗ページ、およびログアウト ページを選択するための 3 つのドロップダウン リストが表示されます。これらすべてのオプションについてカスタマイズしたページを定義する必要はありません。カスタマイズしたページを表示しないオプションに対しては、該当するドロップダウン リストで [None] を選択します。 これらのオプションのログイン ページ、ログイン失敗ページ、ログアウト ページは、webauth.tar ファイルとしてコントローラにダウンロードされます。 [External]:認証のためにユーザを外部サーバにリダイレクトします。このオプションを選択する場合、[URL] テキスト ボックスに外部サーバの URL も入力する必要があります。 注　外部 Web 認証は、2106 および 5500 シリーズ コントローラではサポートされていません。 外部認証を行う場合は、[Security] > [AAA] ページで特定の RADIUS サーバまたは LDAP サーバを選択できます。 注　[Security] > [AAA] ページで選択できるように、RADIUS サーバと LDAP サーバを事前に設定しておく必要があります。[RADIUS Authentication Servers] ページ、[TACACS+ Authentication Servers] ページでこれらのサーバを設定できます。 [Web Authentication Type] で [External] を選択した場合は、[Security] > [AAA] を選択し、ドロップダウン リストから RADIUS サーバと LDAP サーバを 3 つまで選択します。 2 番めの(アンカー)コントローラがネットワークで使用中の場合は、このプロセスを繰り返します。

表 2-69　[Controller] > [WLANs] > [WLAN Configuration] > [Security]（続き）

フィールド	説明
AAA Server	
Radius Server Overwrite Interface	WLAN に設定されている動的インターフェイスを経由してクライアントが認証要求を送信する場合にオンにします。[Radius Server Overwrite Interface] オプションを有効にすると、WLC は、その WLAN で設定されているダイナミック インターフェイスを使用して、WLAN のすべての RADIUS トラフィックを送信します。 **注**　[Diagnostic Channel] が有効な場合、[Radius Server Overwrite Interface] を有効にすることはできません。 **注**　[Radius Server Overwrite Interface] オプションは、コントローラ バージョン 7.0.x 以降でサポートされます。 [Enable] チェックボックスをオンにし、RADIUS および LDAP サーバ セクションのドロップダウン リストを使用して、認証およびアカウンティング サーバを選択します。これによって、指定した WLAN のデフォルトの RADIUS サーバが選択され、ネットワークに対して設定されている RADIUS サーバは上書きされます。3 つすべての RADIUS サーバが特定の 1 つの WLAN に対して設定されている場合、優先順位はサーバ 1 が最も高くなります。 LDAP サーバをここで選択しないと、Prime Infrastructure はデータベースのデフォルトの LDAP サーバ順序を使用します。
Interim Update	RADIUS サーバ アカウンティングの暫定アップデートを有効にする場合はオンにします。このチェックボックスをオンにした場合、[Interim Interval] 値を指定します。範囲は 180 ～ 3600 秒で、デフォルト値は 0 です。 **注**　[Interim Interval] は、[Interim Update] を有効にした場合にのみ入力できます。
Local EAP Authentication	有効にする EAP プロファイルをすでに設定している場合は、[Local EAP Authentication] チェックボックスをオンにします。ローカル EAP は、ユーザと無線クライアントがローカルで認証できる認証メソッドです。この方式は、バックエンド システムが妨害されたり、外部認証サーバがダウンした場合でも、ワイヤレス クライアントへの接続を維持できるように、リモート オフィスで使用する目的で設計されています。
Allow AAA Override	AAA Override を有効にした場合で、クライアントにおいて AAA とコントローラ WLAN 認証フィールドが競合しているときは、クライアント認証は AAA サーバにより行われます。この認証の一部として、オペレーティング システムはクライアントをデフォルトの Cisco WLAN ソリューション から、AAA サーバにより返され、コントローラのインターフェイス設定で事前定義された VLAN に移動します（MAC フィルタリング、802.1X、または WPA 動作用に設定されている場合のみ）。すべての場合において、オペレーティング システムは、QoS、および AAA サーバにより提供される ACL がコントローラ インターフェイス設定で事前に定義されている限り、これらも使用します。（この AAA オーバーライドによる VLAN スイッチングは、ID ネットワーキングとも呼ばれます）。 たとえば、企業の WLAN が主に VLAN 2 に割り当てられた管理インターフェイスを使用し、AAA Override が VLAN 100 へのリダイレクトを返す場合、物理ポートが VLAN 100 に割り当てられているかどうかは関係なく、オペレーティング システムは、すべてのクライアント転送を VLAN 100 にリダイレクトします。 AAA Override が無効の場合、すべてのクライアント認証はデフォルトのコントローラの認証パラメータ設定となり、コントローラの WLAN にクライアント固有の認証パラメータが含まれていない場合、認証のみ AAA サーバによって行われます。 AAA オーバーライド値は、たとえば RADIUS サーバから取り込まれます。

[Controller] > [WLANs] > [WLAN Configuration] > [QoS]

次の表で、[Design] > [Configuration] > [Feature Design] > [Features and Technologies] > [Controller] > [WLANs] > [WLAN Configuration] > [QoS] にある [Template Detail] の各フィールドについて説明します。

表 2-70　[Controller] > [WLANs] > [WLAN Configuration] > [QoS]

フィールド	説明
Quality of Service（QoS）	[Platinum (voice)]、[Gold (video)]、[Silver (best effort)]、または [Bronze (background)] を選択します。VoIP などのサービスは [Gold] に設定する必要がありますが、テキスト メッセージなど差別的ではないサービスは [Bronze] に設定できます。
Override Per-User Rate Limits	ユーザごとのデータ レート
Average Data Rate	[Average Data Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザごとまたは SSID ごとの TCP トラフィックの平均データ レートを定義します。値 0 は、プロファイルに帯域幅の制限を課しません。
Burst Data Rate	[Burst Data Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザごとまたは SSID ごとの TCP トラフィックのピーク データ レートを定義します。値 0 は、プロファイルに帯域幅の制限を課しません。burst-data-rate は average-data-rate 以上でなければなりません。それ以外の場合、QoS ポリシーにより、ワイヤレス クライアントとのトラフィックがブロックされることがあります。
Average Real-Time Rate	[Average Real-Time Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザごとまたは SSID ごとの UDP トラフィックの平均リアルタイム レートを定義します。値 0 は、プロファイルに帯域幅の制限を課しません。
Burst Real-Time Rate	[Burst Real-Time Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザごとまたは SSID ごとの UDP トラフィックのピーク リアルタイム レートを定義します。値 0 は、プロファイルに帯域幅の制限を課しません。burst-realtime-rate は average-realtime-rate 以上でなければなりません。それ以外の場合、QoS ポリシーにより、ワイヤレス クライアントとのトラフィックがブロックされることがあります。
Override Per-SSID Rate Limits	SSID ごとのデータ レート
Average Data Rate	[Average Data Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザごとまたは SSID ごとの TCP トラフィックの平均データ レートを定義します。値 0 は、プロファイルに帯域幅の制限を課しません。
Burst Data Rate	[Burst Data Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザごとまたは SSID ごとの TCP トラフィックのピーク データ レートを定義します。値 0 は、プロファイルに帯域幅の制限を課しません。burst-data-rate は average-data-rate 以上でなければなりません。それ以外の場合、QoS ポリシーにより、WLAN のトラフィックがブロックされることがあります。
Average Real-Time Rate	[Average Real-Time Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザごとまたは SSID ごとの UDP トラフィックの平均リアルタイム レートを定義します。値 0 は、プロファイルに帯域幅の制限を課しません。
Burst Real-Time Rate	[Burst Real-Time Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザごとまたは SSID ごとの UDP トラフィックのピーク リアルタイム レートを定義します。値 0 は、プロファイルに帯域幅の制限を課しません。burst-realtime-rate は average-realtime-rate 以上でなければなりません。それ以外の場合、QoS ポリシーにより、WLAN のトラフィックがブロックされることがあります。

表 2-70　[Controller] > [WLANs] > [WLAN Configuration] > [QoS]（続き）

フィールド	説明
WMM Policy	[Disabled]、[Allowed]（クライアントが WLAN と通信できるようにする）、または [Required]（クライアントが通信で WMM を有効にすることを必須とする）を選択します。
7920 AP CAC	Cisco 7920 電話でのサポートを有効にする場合はオンにします。 7920 電話で WLAN に旧バージョンのソフトウェアをサポートさせる場合は、[7920 Client CAC] チェックボックスをオンにして有効にします。コール アドミッション制御（CAC）の制限は、より新しいバージョンのソフトウェアのアクセス ポイントで設定されます。

[Controller] > [WLANs] > [WLAN Configuration] > [Advanced]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [WLANs] > [WLAN Configuration] > [Advanced] にある [Template Detail] の各フィールドについて説明します。

表 2-71　[Controller] > [WLANs] > [WLAN Configuration] > [Advanced]

フィールド	説明
FlexConnect Local Switching	FlexConnect ローカル スイッチングを有効にする場合はオンにします。FlexConnect ローカル スイッチングを有効にすると、FlexConnect のアクセス ポイントは、クライアント認証を処理し、クライアント データ パケットをローカルにスイッチングします。 FlexConnect ローカル スイッチングは、Cisco 1130/1240/1250 シリーズのアクセス ポイントに対してだけ適用可能です。これは、L2TP または PPTP 認証ではサポートされていません。また、WLAN ID 9 ～ 16 には適用できません。
FlexConnect Local Auth	FlexConnect ローカル認証を有効にする場合はオンにします。 ローカル認証は、ラウンドトリップ遅延が 100 ms を超えず、最大伝送ユニット（MTU）が 500 バイトを下回らない、最小帯域幅が 128 kbps のリモート オフィス設定の基準を維持できない場合に役立ちます。ローカル スイッチングでは、認証機能はアクセス ポイント自体に存在します。そのため、ローカル認証によって、ブランチ オフィスの遅延要件が軽減されます。 **注**　ローカル認証は、ローカル スイッチング モードの FlexConnect AP の WLAN のみで有効にできます。 ローカル認証は、次のシナリオではサポートされません。 • FlexConnect ローカル認証を有効にした WLAN では、ゲスト認証は実行できません。 • RRM 情報は、FlexConnect ローカル認証を有効にした WLAN のコントローラでは使用不可です。 • ローカル RADIUS はサポートされません。 • クライアントが認証されると、グループの WLC およびその他の FlexConnect でクライアント情報が更新された後で、ローミングがサポートされます。
Learn Client IP Address	H-REAP ローカル スイッチングを有効にすると、[Learn Client IP Address] チェックボックスがデフォルトで有効になります。ただし、クライアントが Fortress レイヤ 2 暗号化を使用するように設定されている場合は、コントローラがそのクライアント IP アドレスを知ることができないので、コントローラはクライアントの接続を定期的に切断します。コントローラがクライアント IP アドレスを知らなくてもクライアント接続を維持できるように、このオプションを無効にしてください。このオプションを無効にできるのは、H-REAP ローカル スイッチングを行うように設定されているときだけです。H-REAP 中央スイッチングを行う場合は、無効にすることはできません。

表 2-71　[Controller] > [WLANs] > [WLAN Configuration] > [Advanced]（続き）

フィールド	説明
Diagnostic Channel	選択して診断チャネル機能を有効にするか、そのままにして機能を無効にします。診断チャネル機能により、WLAN とのクライアント通信に関する問題のトラブルシューティングが可能になります。問題のあるクライアントにより診断チャネルが開始されると、通信への障害物が最も少なく、最も堅牢な通信方法が提供されます。
Aironet IE	この WLAN の Aironet 情報要素（IE）のサポートを有効にする場合はオンにします。Aironet IE のサポートが有効になっている場合、アクセス ポイントは、Aironet IE 0x85（アクセス ポイント名、ロード、アソシエートされたクライアントの番号などを含む）をこの WLAN のビーコンやプローブ応答に格納して送信します。また、アクセス ポイントが再アソシエーション要求内の Aironet IE 0x85 を受信する場合、コントローラは、Aironet IEs 0x85 および 0x95（コントローラの管理 IP アドレスおよびアクセス ポイントの IP アドレスを含む）を再アソシエーション要求に格納して送信します。
IPv6	[IPv6] チェックボックスをオンにします。同じ WLAN 上で IPv6 ブリッジおよび IPv4 Web 認証を設定できます。
Session Timeout	クライアント セッションが再認可を必要とせずに続行できる最大時間を設定する場合はオンにします。
Coverage Hole Detection	この WLAN で Coverage Hold Detection（CHD）を有効または無効にするか選択します。デフォルトでは、CHD は、コントローラのすべての WLAN で有効です。WLAN で CHD を無効にした場合、カバレッジ ホールの警告はコントローラに送信されますが、カバレッジ ホールを解消するためのそれ以外の処理は行われません。この機能は、モバイル利用率の高いゲストが短期間だけネットワークに接続するゲスト WLAN で役に立ちます。
Override Interface ACL	[Override Interface ACL] ドロップダウン リストは、定義済みのアクセス コントロール リスト（ACL）のリストを提供します。リストから ACL を選択すると、WLAN はその ACL を WLAN に関連付けます。ACL の選択はオプションで、このフィールドのデフォルトは、[None] です。
Peer to Peer Blocking	すべての WLAN にステータスを適用するのではなく、WLAN ごとにピアツーピア ブロックを設定できます。[Peer to Peer Blocking] ドロップダウン リストから、次のいずれかを選択します。 • [Disable]：ピアツーピア ブロックは無効にされています。トラフィックは可能な場合はローカルでブリッジされます。 • [Drop]：パケットは廃棄されます。 • [Forward Up Stream]：パケットはアップストリーム VLAN 上に転送され、そのパケットをどうするかが決定されます。 **注**　ローカルでスイッチされるクライアントの場合、転送アップ ストリームはバージョン 7.2.x のコントローラからのドロップと同じになります。 WLAN の FlexConnect ローカル スイッチングが有効になっている（トラフィックがコントローラを通過するのを防ぐ）場合は、このドロップダウン リストが灰色になります。 **注**　ピアツーピア ブロッキングは、マルチキャスト トラフィックには適用されません。

表 2-71　[Controller] > [WLANs] > [WLAN Configuration] > [Advanced]（続き）

フィールド	説明
Wi-Fi Direct Clients Policy	次のいずれかのオプションを選択します。 • [Disabled]：WLAN の Wi-Fi Direct クライアント ポリシーを無効にして、すべての Wi-Fi Direct 対応クライアントを認証解除します。デフォルトでは無効になっています。 • [Allow]：Wi-Fi Direct クライアントとインフラストラクチャ WLAN とのアソシエーションを許可します。 • [Not-Allow]：Wi-Fi Direct クライアントとインフラストラクチャ WLAN とのアソシエーションを禁止します。 **注**　Wi-Fi Direct クライアント ポリシーは、ローカル モードの AP が含まれる WLAN のみに適用できます。 **注**　Wi-Fi Direct クライアント ポリシーは、バージョン 7.2.x 以降のコントローラのみに適用できます。
Client Exclusion	自動的なクライアントの除外を有効にする場合は、このチェックボックスをオンにします。クライアントの除外を有効にする場合、無効となるクライアント マシンのタイムアウト値を秒単位で設定することも必要です。クライアント マシンは MAC アドレスで除外され、そのステータスは監視できます。0 のタイムアウト設定は、クライアントを再度有効にするには管理制御が必要であることを示します。 **注**　セッションのタイムアウトが設定されていない場合、除外されたクライアントはそのまま残り、除外された状態からタイムアウトすることはありません。除外機能が無効であることを意味するのではありません。
Passive Client	[Maximum Clients] テキスト ボックスに、WLAN に関連付けられるクライアントの最大数を入力します。有効な範囲は 0 ～ 7000 です。デフォルト値は 0 です **注**　値を 0 にすると、WLAN に関連付けられるクライアント数が無限になります。
Static IP Tunneling	[Static IP Tunneling] チェックボックスをオンして、スタティック IP クライアントのダイナミック アンカリングを有効にします。
Media Session Snooping	この機能により、アクセス ポイントは音声コールの確立、終了、および失敗を検出し、それをコントローラおよび Prime Infrastructure にレポートできます。WLAN ごとに有効化または無効化できます。 メディア セッション スヌーピングが有効な場合、この WLAN をアドバタイズするアクセス ポイント無線は、Session Initiation Protocol（SIP）音声パケットをスヌープします。ポート番号 5060 に宛てた、またはポート番号 5060 からのパケットはいずれも、詳細検査の対象として考慮されます。アクセス ポイントは、Wi-Fi マルチメディア（WMM）および非 WMM クライアントがコールを確立中か、すでにアクティブなコール上にあるか、またはコールの終了処理中であるかをトラッキングし、コントローラに対して主要なコール イベントを通知します。

表 2-71　[Controller] > [WLANs] > [WLAN Configuration] > [Advanced]（続き）

フィールド	説明
KTS based CAC	[KTS based CAC] チェックボックスをオンにして、WLAN ごとの KTS ベース CAC サポートを有効にします。 WLC は、TSPEC ベースの CAC および SIP ベースの CAC をサポートします。ただし、異なる CAC のプロトコルで稼働する特定の電話があります。これらは、KTS（Key Telephone System）をベースとします。CAC および KTS ベースの SIP クライアントをサポートするには、WLC はこのプロトコルの一部として、特定のその他のメッセージを処理して送信することに加えて、これらのクライアントからの帯域幅要求メッセージを理解して処理し、AP 無線上に要求された帯域幅を割り当てる必要があります。 **注**　KTS CAC 設定は、コントローラ ソフトウェア リリース 7.2.x を実行する Cisco 5508、7500、WISM2、2500 コントローラのみでサポートされています。この機能は、Cisco 4400 シリーズ コントローラではサポートされません。
NAC State	[SNMP NAC] または [Radius NAC] を選択します。検出された SIP エラーにより、クライアントのトラブルシューティングおよびアラーム画面に表示されるトラップが生成されます。コントローラはアウトオブバンドの NAC アプライアンスと統合できます。NAC アプライアンスは、クライアントが分析および解除されるまでデータ パス内に保持されます。アウトオブバンド モードでは NAC アプライアンスのトラフィック負荷が削減されるので、NAC 処理の集中化が可能になります。
Scan Defer Priority	[Off-Channel Scanning Defer] は、ノイズや干渉など代替チャネル選択に関する情報を収集する RRM を使用するときに重要となります。また、[Off-Channel Scanning Defer] は、不正検出を行います。[Off-Channel Scanning Defer] を提供する必要があるデバイスは、可能な限り、同じ WLAN を使用する必要があります。このようなデバイスが多くある場合（この機能を使用して Off-Channel Defer スキャンが完全に無効化されている可能性があります）、モニタ アクセス ポイントや、この WLAN が割り当てられていない同じ位置にあるその他のアクセス ポイントなど、代わりにローカル AP で [Off-Channel Scanning Defer] を実装する必要があります。 QoS ポリシー（ブロンズ、シルバー、ゴールド、プラチナ）の WLAN への割り当ては、クライアントからアップリンクでどのように受信されたかに関係なく、パケットがアクセス ポイントからのダウンリンク接続でどのようにマーキングされるかに影響します。UP=1,2 は最低の優先順位で、UP=0,3 はその次に高い優先順位です。各 QoS ポリシーのマーキング結果は次のとおりです。 • ブロンズは、すべてのダウンリンク トラフィックを UP=1 にマーキングします。 • シルバーは、すべてのダウンリンク トラフィックを UP=0 にマーキングします。 • ゴールドは、すべてのダウンリンク トラフィックを UP= 4 にマーキングします。 • プラチナは、すべてのダウンリンク トラフィックを UP= 6 にマーキングします。 優先順位引数をクリックして [Scan Defer Priority] を設定し、[Scan Defer Interval] テキスト ボックスに時間をミリ秒単位で設定します。有効値の範囲は 0 ～ 60000 です。デフォルト値は 100 ミリ秒です。

表 2-71　[Controller] > [WLANs] > [WLAN Configuration] > [Advanced]（続き）

フィールド	説明
DTIM Period	802.11a/n ネットワークおよび 802.11b/g/n ネットワークの場合、Lightweight アクセス ポイントは、Delivery Traffic Indication Map（DTIM）と同期する一定間隔でビーコンをブロードキャストします。アクセス ポイントでビーコンがブロードキャストされると、DTIM period で設定した値に基づいて、バッファされたブロードキャスト フレームおよびマルチキャスト フレームが送信されます。この機能により、ブロードキャスト データやマルチキャスト データが予想されると、適切なタイミングで省電力クライアントを再起動できます。 通常、DTIM の値は 1（ブロードキャスト フレームおよびマルチキャスト フレームはビーコンのたびに送信）または 2（ビーコン 1 回おきに送信）のいずれかに設定されます。たとえば、802.11a/n または 802.11b/g/n のネットワークのビーコン期間が 100ms で DTIM 値が 1 に設定されていると、アクセス ポイントは、バッファされたブロードキャスト フレームおよびマルチキャスト フレームを毎秒 10 回送信します。ビーコン期間が 100ms で DTIM 値が 2 に設定されていると、アクセス ポイントは、バッファされたブロードキャスト フレームおよびマルチキャスト フレームを毎秒 5 回送信します。ブロードキャスト フレームおよびマルチキャスト フレームの頻度を考慮して、VoIP を含むアプリケーションに適したいずれかの設定を使用できます。 ただし、802.11a/n または 802.11b/g/n のすべてのクライアントで省電力モードが有効になっている場合は、DTIM 値を最大 255 まで設定できます（ブロードキャスト フレームおよびマルチキャスト フレームは 255 回のビーコンで 1 回送信）。クライアントは DTIM 期間に達したときのみリッスンする必要があるため、ブロードキャストとマルチキャストをリッスンする頻度を少なく設定することで、結果的にバッテリー寿命を長くできます。たとえば、ビーコン期間が 100ms で DTIM 値が 100 に設定されていると、アクセス ポイントは、バッファされたブロードキャスト フレームおよびマルチキャスト フレームを 10 秒おきに送信するので、省電力クライアントを再起動してブロードキャストとマルチキャストをリッスンするまでのスリープ時間が長くなり、結果的にバッテリー寿命が長くなります。 多くのアプリケーションでは、ブロードキャスト メッセージとマルチキャスト メッセージとの間隔を長くすると、プロトコルとアプリケーションのパフォーマンスが低下します。省電力クライアントをサポートしている 802.11a/n ネットワークおよび 802.11b/g/n ネットワークでは、DTIM 値を小さく設定することを推奨します。 [DTIM Period] の下の [802.11a/n] フィールドと [802.11b/g/n] フィールドに 1 ～ 255 までの値を入力します。デフォルト値は 1（ブロードキャスト フレームおよびマルチキャスト フレームはビーコンのたびに送信）です。
DHCP Server	DHCP サーバを上書きするには、このチェックボックスをオンにします。別のフィールドが表示されます。このフィールドに DHCP サーバの IP を入力します。一部の WLAN 設定では、これは必須です。有効な 3 つの設定は、次のとおりです。 • [DHCP Required and a valid DHCP server IP address]：すべての WLAN クライアントは DHCP サーバから IP アドレスを取得します。 • [DHCP is not required and a valid DHCP server address]：すべての WLAN クライアントは、DHCP サーバから IP アドレスを取得するか、スタティック IP アドレスを使用します。 • [DHCP not required and DHCP server IP address 0.0.0.0]：すべての WLAN クライアントは強制的にスタティック IP アドレスを使用します。すべての DHCP 要求はドロップされます。 DHCP のアドレス割り当てを要求した後に DHCP サーバの IP アドレスの入力を選択できません。

表 2-71　[Controller] > [WLANs] > [WLAN Configuration] > [Advanced]（続き）

フィールド	説明
MFP Signature Generation	この WLAN に関連付けられたアクセス ポイントによって送信された 802.11 管理フレームのシグニチャ生成を有効にする場合はオンにします。シグニチャ生成によって、侵入者による送信された管理フレームへの変更が、確実に検出および報告されます。
MFP Client Protection	コントローラの個々の WLAN の設定に[Enabled]、[Disabled]、または [Required] を選択します。インフラストラクチャ MFP が有効でない場合、このドロップダウン リストは使用できません。 **注**　[Enabled] パラメータは、WLC グラフィカル ユーザ インターフェイスの [MFP Client Protection] ドロップダウン リストで選択する [Optional] パラメータと同じです。 **注**　クライアント側 MFP は、Cisco Compatible Extensions（バージョン 5 以降）クライアントをサポートするよう設定されている WLAN でだけ使用でき、WPA2 が最初に設定されている必要があります。
DTIM Period	ビーコン間隔の値を 1 ～ 255 の範囲で入力します。コントローラは、間隔として入力された値に基づいて、この WLAN の DTIM パケットを送信します。 **注**　DTIM 設定は、ゲスト LAN には適していません。
Local Client Profiling	WLAN に関連付けられたすべてのクライアントのプロファイリングを有効または無効にする場合は、このチェックボックスをオンにします。 **注**　FlexConnect ローカル認証では、クライアント プロファイリングはサポートされていません。 **注**　クライアント プロファイリングは、[DHCP Address Assignment] チェックボックスをオンにした場合のみ設定できます。
PMIP Mobility	モビリティ タイプを次のオプションから選択します。 • [None]：簡易 IP を使用して WLAN を設定します。 • [Mixed]：簡易 IP および PMIPv6 を使用して WLAN を設定します。 • [PMIPv6]：PMIPv6 のみを使用して WLAN を設定します。

[Controller] > [WLANs] > [WLAN Configuration] > [HotSpot]

モバイル コンシェルジュは、外部ネットワークで相互運用できるように 802.1X 対応クライアントを有効にするソリューションです。モバイル コンシェルジュ機能は、クライアントにサービスのアベイラビリティに関する情報を提供し、使用可能なネットワークをアソシエートするのに役立ちます。

ネットワークから提供されるサービスは、次の 2 つのプロトコルに大きく分類できます。

- 802.11u MSAP
- 802.11u HotSpot 2.0

モバイル コンシェルジュには、次のガイドラインと制限事項が適用されます。

- モバイル コンシェルジュは FlexConnect アクセス ポイントではサポートされません。
- 802.11u 設定アップロードはサポートされません。設定のアップグレードを実行し、設定をコントローラにアップロードすると、WLAN の HotSpot の設定は失われます。

モビリティ コンシェルジュ（802.11u）グループを作成するには、[Configuration] > [Templates] > [Features and Technologies] > [Controller]> [WLANs] > [WLAN Configuration] > [Hot Spot] を選択します。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [WLANs] > [WLAN Configuration] > [HotSpot] にある [Template Detail] の各フィールドについて説明します。

表 2-72　[Controller] > [WLANs] > [WLAN Configuration] > [HotSpot]

フィールド	説明
General	
802.11u Status	WLAN で 802.11u を有効にする場合はオンにします。 • ドロップダウン リストから、[HESSID] フィールドに Homogenous Extended Service Set Identifier 値を入力します。HESSID は、HESS を識別する 6 オクテットの MAC アドレスです。
Internet Access	この WLAN を有効にしてインターネット サービスを提供する場合はオンにします。
Network Type	この WLAN に設定する 802.11u を最も適切に説明するネットワーク タイプを次の中から 1 つ選択します。 • Private Network • Private Network with Guest Access • Chargeable Public Network • Free Public Network • Emergency Services Only Network • Personal Device Network • Test or Experimental • Wildcard
Network Auth Type	このネットワークの 802.11u パラメータ用に設定する認証タイプを選択します。 • Not configured • Acceptance of Terms and Conditions • Online Enrollment • HTTP/HTTPS Redirection
OUI List	次の詳細を入力します。 • OUI name • Is Beacon • OUI Index [Add] を選択して、OUI(組織固有識別子)エントリをこの WLAN に追加します。 • グループ ボックス内
Domain List	次の詳細を入力します。 • [Domain Name]:802.11 アクセス ネットワークで稼働するドメイン名。 • [Domain Index]:ドロップダウン リストからドメイン インデックスを選択します。 [Add] を選択して、ドメイン エントリをこの WLAN に追加します。

表 2-72　[Controller] > [WLANs] > [WLAN Configuration] > [HotSpot]（続き）

フィールド	説明
OUI List	次の詳細を入力します。 • [Realm Name]：レルム名。 • [Realm Index]：レルム インデックス。 [Add] を選択して、ドメイン エントリをこの WLAN に追加します。
MSAP	サービス アドバタイズメントを有効にする場合はオンにします。
Server Index	MSAP を有効にした場合は、サーバ インデックスを提供する必要があります。この WLAN のサーバ インデックスを入力します。サーバのインデックス フィールドによって、BSSID を使用して到達可能である場所を提供する MSAP サーバ インスタンスを一意に識別します。 **注**　MSAP（Mobility Services Advertisement Protocol）は、ネットワーク接続を確立するためのポリシー セットを使用して設定されたモバイル デバイスで主に使用するために設計されています。これらのサービスは、上位層サービスを提供するデバイス、つまりサービス プロバイダー経由で有効にされるネットワーク サービス向けです。サービス アドバタイズメントは、MSAP を使用して、Wi-Fi アクセス ネットワークへのアソシエーションの前にサービスをモバイル デバイスに提供します。この情報はサービス アドバタイズメントで伝送されます。シングルモードまたはデュアルモード モバイル デバイスは、アソシエーションの前にサービス ネットワークをネットワークにクエリーします。デバイスによるネットワークの検出および選択機能では、ネットワークに join する判断においてサービス アドバタイズメントを使用する場合があります。
HotSpot2 Enable	HotSpot2 を有効にします。
WAN Link Status	リンク ステータスを選択します。
WAN Symmetric Link Status	対称リンク ステータス。たとえば、アップリンクとダウンリンクに異なる速度または同じ速度を設定できます。
Down Link Speed	ダウンリンク速度。最大値は 4,194,304 kbps です。
Up Link Speed	アップリンク速度。最大値は 4,194,304 kbps です。
Operator Name List	次のことを指定します。 • [Operator Name]：802.11 オペレータの名前を指定します。 • [Operator Index]：オペレータ インデックスを選択します。指定できる範囲は 1 ～ 32 です。 • [Language Code]：言語を定義する ISO-14962-1997 エンコード文字列。この文字列は 3 文字の言語コードです。 [Add] を選択して、オペレータの詳細を追加します。
Port Config List	次のことを指定します。 • [IP Protocol]：有効にしたい IP プロトコル。次のオプションは、ESP、FTP、ICMP、および IKEV2 です。 • [Port No]：この WLAN で有効になっているポート番号。 • [Status]：ポートのステータス。

[Controller] > [mDNS]

マルチキャスト DNS(mDNS)サービス検出では、ローカル ネットワーク上のサービスをアナウンスし、検出するための手段を提供します。mDNS は、IP マルチキャストで DNS クエリを実行します。mDNS は ゼロ コンフィギュレーション IP ネットワーキングがをサポートします。

mDNS テンプレートを作成するときには、次のガイドラインおよび制限事項に従ってください。

- mDNS サービスが 1 つ以上のプロファイルにマップされている場合、その mDNS サービスは削除できません。
- プロファイル名およびサービス名は最大 31 文字です。
- サービス文字列の長さは最大 255 文字です。
- デフォルト プロファイル(default-mdns-profile)は削除できません。
- プロファイルがインターフェイス、インターフェイス グループ、または WLAN にマップされている場合、それらのプロファイルは削除できません。
- mDNS サービスがインターフェイス、インターフェイス グループ、または WLAN にマップされている場合、プロファイルからそれらの mDNS サービスを削除できません。新しいサービスを追加できます。
- mDNS テンプレートを作成して適用すると、コントローラの現在の設定が上書きされます。
- FlexConnect ローカル スイッチングが有効になっている場合、WLAN の mDNS スヌーピングは有効にできません。
- AP Management が有効の場合、インターフェイスに mDNS プロファイルをアタッチできません。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [mDNS] > [mDNS] にある [Template Detail] の各フィールドについて説明します。

表 2-73　[Controller] > [mDNS] > [mDNS]

フィールド	説明
[Services] タブ	このタブのフィールドを使用して、グローバル mDNS パラメータを設定し、Master Services データベースを更新します。
MDNS Global Snooping	mDNS パケットのスヌーピングを有効にする場合はオンにします。 **注**　コントローラは mDNS スヌーピングを有効にしても、IPv6 mDNS パケットをサポートしません。
Query Interval(10-120)	設定可能な分単位の mDNS クエリー間隔。この間隔は、WLC によって、サービス アドバタイズメントを自動的に送信しないサービスに対して、そのサービスが開始された後に定期的な mDNS クエリー メッセージを送信するために使用されます。範囲は 10 ～ 120 分です。デフォルト値は 15 分です。
Master Services	クエリーが可能なサポート対象のサービスのリスト。
Master Service Name	mDNS サービスの名前。
Service String	mDNS サービスに関連付けられた一意の文字列。たとえば、_airplay._tcp.local. は、AppleTV に関連付けられたサービス文字列です。
Query Status	サービスに mDNS クエリーを有効にするには、このチェックボックスをオンにします。 **注**　定期的な mDNS クエリー メッセージは、クエリーのステータスが有効な場合だけ、WLC によって、サービスに対して設定されたクエリー間隔で送信されます。それ以外の場合、サービスは、クエリーのステータスが無効になっているその他のサービス(たとえば AppleTV)に自動的にアドバタイズする場合があります。

表 2-73　[Controller] > [mDNS] > [mDNS]（続き）

フィールド	説明
[Profiles] タブ	このタブを使用して、コントローラに設定されている mDNS プロファイルを表示し、新しい mDNS プロファイルを作成します。新しいプロファイルを作成した後、インターフェイス グループ、インターフェイス、または WLAN にプロファイルをマッピングする必要があります。 クライアントはプロファイルに関連付けられたサービスだけのサービス アドバタイズメントを受信します。コントローラはインターフェイス グループに関連付けられたプロファイルに最高の優先順位を与えます。次にインターフェイス プロファイル、WLAN プロファイルが続きます。各クライアントは、優先順位に従ってプロファイルにマップされます。 デフォルトでは、コントローラに mDNS プロファイル、デフォルト mdns プロファイルがあります。このデフォルト プロファイルは削除できません。
Profile Name	mDNS プロファイルの名前。最大 16 個のプロファイルを作成できます。
Mapped Services	mDNS プロファイルにマップするサービスを選択します（チェックボックスを使用）。

[Interfaces Templates] フィールドの説明

次に、[Configuration] > [Templates] > [Features and Technologies] > [Interfaces] > [Cellular] にあるページの各フィールドについて説明します。

- [Interfaces] > [Cellular Profile]（2-86 ページ）
- [Interfaces] > [GSM Profile]（2-87 ページ）

[Interfaces] > [Cellular Profile]

注　UMTS、GSM、HSPA、または HSPA+R7 モデムでセルラー プロファイル テンプレートを展開するには、ルータに GSM プロファイル（[Interfaces] > [GSM Profile]（2-87 ページ））が設定されている必要があります。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Interfaces] > [Cellular] > [Cellular Profile] にある [Template Detail] の各フィールドについて説明します。

表 2-74　[Interfaces] > [Cellular] > [Cellular Profile]

フィールド	説明
Validation Criteria	
Device Type	ドロップダウン リストから、デバイス タイプを選択します。
Interface Details	
Cellular Interface	セルラー インターフェイスの名前を入力します。固定プラットフォーム ルータ（8xx）の場合は、常に Cellular 0、モジュラ プラットフォームの場合は、セルラー スロット/サブ スロットまたはポートの形式です。例えば、Cellular 0/1/0 などです。

表 2-74　[Interfaces] > [Cellular] > [Cellular Profile]（続き）

フィールド	説明
Define this cellular interface as	次のオプションのいずれかを選択し、セルラー インターフェイスを設定します。 • Primary WAN Interface • Backup WAN Interface
Primary Interface	プライマリ インターフェイスの詳細情報を入力します。このフィールドは、[Define this cellular interface as] が [Backup WAN Interface] に設定されているときに表示されます。
Routemap Configuration	
[Route Map] タグ	ルート マップを識別する一意の名前を入力します。
Sequence Number	ルート マップの条件を定義する数値を入力します。
Action	デフォルトでは、このフィールド値は [Permit] に設定されています。
Access List	対象となるトラフィックを検査するため、ルート マップに関連付けられたアクセス リストの詳細情報を入力します。ACL は、拡張 ACL である必要があり、名前付きの ACL であってもかまいません。
First Hop Interface	(読み取り専用)ユーザがプライマリ インターフェイスを入力したときに詳細が自動的に挿入されます。
IP SLA Configuration	
Target Address	接続が確認されるサーバの IP アドレスを入力します。このサーバは、サービス レベル契約(SLA)の一部として特定されます。
Timeout Value	ping 要求ごとにタイムアウト値をミリ秒単位で入力します。
Time Interval	ping が生成される間隔を入力します。
Dialer Configuration	
Persistent Data Connection	永続的なデータ接続を有効にするには、[Yes] を選択します。
Associate Dialer	関連ダイヤラを入力します。このフィールドは、[Persistent Data Connection] を [Yes] に設定した場合に表示されます。
Dialer Idle Timeout	ダイヤラのアイドル タイムアウトを入力します。このフィールドは、[Persistent Data Connection] を [No] に設定した場合に表示されます。
Chat-Script Configuration	
Chat-Script Name	セルラー モデムがダイヤル アウトし、トラフィックを開始する文字列値を入力します。
Timeout Value	Cisco IOS デバイスがモデムからの応答を待機するために使用するタイムアウト値を入力します。Cisco IOS が期待している応答を取得できない場合やセルラー モデムからの応答がない場合、コールは失敗します。

[Interfaces] > [GSM Profile]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Interfaces] > [Cellular] > [GSM Profile] にある [Template Detail] の各フィールドについて説明します。

表 2-75　[Interfaces] > [Cellular] > [GSM Profile]

フィールド	説明
Device Type	ドロップダウン リストから、デバイス タイプを選択します。
Template Detail	
Cellular Interface	最大 16 個のプロファイルをサポートする一方で、一度に 1 つのみをアクティブ化する Cisco ワイヤレス WAN インターフェイスを入力します。一般に、デフォルトではプロファイル番号 1 が選択されます。
Access Point Name (APN; アクセス ポイント名)	モバイル データ ユーザが通信するパケット データ ネットワーク(PDN)を識別する名前を入力します。一般に、ユーザがセルラー モデムを購入した時点で、APN はサービス プロバイダーによって共有されます。
Profile Number	ドロップダウン リストから、プロファイル番号を選択します。
PDP Type	ドロップダウン リストからパケット データ プロトコル(PDP)タイプを選択します。PDP は、モバイルやネットワークなどのユーザ機器が IP パケットをやり取りできるパケット データ接続を提供します。 選択可能な PDP タイプは次のとおりです。 • IPv4(デフォルト) • PPP
Authentication	サービス プロバイダーが使用する認証のタイプを選択します。CHAP 認証は PAP 認証よりもセキュアです。
Username Password	CHAP 認証、または PAP 認証では、インターネット サービス プロバイダーまたはネットワーク管理者が付与したユーザ名を入力します。

[Security Templates] フィールドの説明

次に、[Configuration] > [Templates] > [Features and Technologies] > [Security] にあるページの各フィールドについて説明します。

- [Security] > [VPN Components](2-89 ページ)
- [Security] > [Zone Based Firewall](2-93 ページ)
- [Security] > [DMVPN](2-95 ページ)
- [Security] > [Easy VPN Remote](2-99 ページ)
- [Security] > [Easy VPN Server](2-102 ページ)
- [Security] > [Easy VPN Server Proxy Setting](2-105 ページ)
- [Security] > [GETVPN-GroupMember](2-106 ページ)
- [Security] > [GETVPN-KeyServer](2-108 ページ)
- [Security] > [ScanSafe](2-110 ページ)

[Security] > [VPN Components]

次に、[Configuration] > [Templates] > [Features and Technologies] > [Security] > [VPN Components] の各フィールドについて説明します。

- [Security] > [VPN Components] > [IKE Policies](2-89 ページ)
- [Security] > [VPN Components] > [IKE Settings](2-90 ページ)
- [Security] > [VPN Components] > [IPSec Profile](2-91 ページ)
- [Security] > [VPN Components] > [Pre-shared Keys](2-92 ページ)
- [Security] > [VPN Components] > [RSA-Keys](2-92 ページ)
- [Security] > [VPN Components] > [Transform Sets](2-92 ページ)

[Security] > [VPN Components] > [IKE Policies]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Security] > [VPN Components] > [IKE Policies] にある [Template Detail] の各フィールドについて説明します。

表 2-76　[Security] > [VPN Components] > [IKE Policies]

フィールド	説明
IKE Policies	
Priority	IKE プロポーザルのプライオリティ値を入力します。このプライオリティ値によって、共通の SA の検出試行時に、ネゴシエーションする 2 つのピアを比較することで、IKE プロポーザルの順序が決定します。リモート IPsec ピアが、最初のプライオリティ ポリシーで選択されているパラメータをサポートしていない場合、デバイスは、次に低いプライオリティ番号を持つポリシーで定義されているパラメータの使用を試行します。 範囲は 1 ～ 10000 です。値が小さいほど、プライオリティが高くなります。
Authentication	[Authentication] ドロップダウン リストから、次のオプションのいずれかを選択します。 • [Pre_SHARE]:事前共有キーを使用して認証が実行されます。 • [RSA_SIG]:デジタル署名を使用して認証が実行されます。
D-H Group	Diffie-Hellman(D-H)グループは、2 つの IPsec ピア間の共有秘密を互いに送信することなく実行するために使用されます。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。2 つのピアに、一致する係数グループが設定されている必要があります。 [Diffie-Hellman Group] ドロップダウン リストから、次のオプションのいずれかを選択します。 • [1]:Diffie-Hellman グループ 1(768 ビット係数)。 • [2]:Diffie-Hellman グループ 2(1024 ビット係数)。 • [5]:Diffie-Hellman グループ 5(1536 ビット係数。128 ビット キーの保護に推奨される)。

表 2-76　[Security] > [VPN Components] > [IKE Policies]（続き）

フィールド	説明
暗号化	[Encryption] ドロップダウン リストから暗号化アルゴリズムの 1 つを選択します。 • [AES-128]：128 ビット キーを使用する高度暗号化規格（AES）に従って暗号化を実行します。 • [AES-192]：192 ビット キーを使用する AES に従って暗号化を実行します。 • [AES-256]：256 ビット キーを使用する AES に従って暗号化を実行します。 • [DES]：56 ビット キーを使用するデータ暗号規格（DES）に従って暗号化を実行します。 • [3DES]：56 ビット キーを使用して暗号化を 3 回実行します。3DES は DES よりもセキュアですが、暗号化と復号化には、より多くの処理を必要とします。ただし、AES に比べるとセキュリティは低くなります。 **注**　このオプションを使用するには 3DES のライセンスが必要です。
Hash	ハッシュ アルゴリズムのドロップダウン リストを選択します。このハッシュ アルゴリズムによって、メッセージの整合性の確保に使用されるメッセージ ダイジェストが作成されます。次のオプションがあります。 • [SHA (Secure Hash Algorithm)]：160 ビットのダイジェストを生成します。SHA には、総当たり攻撃に対して、MD5 よりも高い耐性が備えられています。 • [MD5 (Message Digest 5)]：128 ビットのダイジェストを生成します。MD5 では、処理時間が SHA よりも少なくなります。
IKE lifetime	SA のライフタイムを秒単位で入力します。このライフタイムを超えると、SA の期限が切れ、2 つのピア間で再ネゴシエーションを行う必要があります。一般的に、一定の限度に達するまで、ライフタイムが短いほど、IKE ネゴシエーションがセキュアになります。ただし、ライフタイムが長いと、今後の IPsec セキュリティ アソシエーションのセットアップが、短いライフタイムの場合よりも迅速に行われます。 範囲は 60 ～ 86400 です。デフォルト値は 86400 です。

[Security] > [VPN Components] > [IKE Settings]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Security] > [VPN Components] > [IKE Settings] にある [Template Detail] の各フィールドについて説明します。

表 2-77　[Security] > [VPN Components] > [IKE Settings]

フィールド	説明
IKE Settings	
Enable IKE	IKE をグローバルに有効にするには、[Enable IKE] チェックボックスをオンにします（デフォルトでは、IKE は有効になっています）。インターフェイスごとに IKE を有効にする必要はなく、ルータですべてのインターフェイスに対してグローバルに有効にすることができます。 IP Security（IPsec）の実装に IKE を使用しない場合は、すべての IPsec ピアに対して IKE を無効にすることができます。あるピアに対して IKE を無効にする場合は、すべての IPsec ピアに対して IKE を無効にする必要があります。

表 2-77　[Security] > [VPN Components] > [IKE Settings]（続き）

フィールド	説明
Enable Aggressive Mode	Internet Security Association and Key Management Protocol（ISAKMP）アグレッシブ モードを有効にするには、[Enable Aggressive Mode] チェックボックスをオンにします。このアグレッシブ モードを無効にした場合、デバイスに対するすべてのアグレッシブ モード要求と、デバイスから出されたすべてのアグレッシブ モード要求がブロックされます。
IKE Identity	[IKE identity] ドロップダウン リストからいずれかのオプションを選択します。 ISAKMP 識別情報は、事前共有キーまたは RSA 署名の認証を指定した場合は常に設定されます。原則として、ピアの識別情報はすべて同じ方法で（IP アドレスまたはホスト名のいずれかで）設定してください。次のオプションがあります。 • [IP Address]：ISAKMP 識別情報を、IKE ネゴシエーションのときにリモート ピアと通信するために使用するインターフェイスの IP アドレスに設定します。 • [Distinguished Name]：ISAKMP 識別情報を、ルータ証明書の識別名（DN）に設定します。 • [HOSTNAME]：ISAKMP 識別情報を、ドメイン名と連結されたホスト名（例：myhost.example.com）に設定します。
Enable Dead Peer Detection (DPD)	ゲートウェイがピアに Dead Peer Detection（DPD）メッセージを送信できるようにします。DPD は、ルータが IKE ピアの活性を照会するために使用できるキープアライブ スキームです。
Keepalive	DPD メッセージの間隔を、[DPD Keepalive] フィールドに秒数で指定します。範囲は 10 ～ 3600 です。
Retry	DPD 再試行時に DPD メッセージが失敗した場合の再試行間隔を秒単位で指定します。範囲は 2 ～ 60 です。

[Security] > [VPN Components] > [IPSec Profile]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Security] > [VPN Components] > [IPSec Profile] にある [Template Detail] の各フィールドについて説明します。

表 2-78　[Security] > [VPN Components] > [IPSec Profile]

フィールド	説明
Name	この IPsec プロファイルの名前を入力します。プロファイルを編集する場合、IPsec プロファイルの名前を編集することはできません。
Description	追加または編集している IPsec プロファイルの説明を追加します。
Transform Sets	トランスフォーム セット名を入力します。トランスフォーム セット（[Security] > [VPN Components] > [Transform Sets]（2-92 ページ）を参照）によって、トンネル上のトラフィックが暗号化されます。
IPSec SA Lifetime (secs)	設定した期間が経過した後に新しい SA を確立するための、[IPSec SA Lifetime] を入力します。この時間は秒数で入力します。範囲は 120 ～ 86400 です。

[Security] > [VPN Components] > [Pre-shared Keys]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Security] > [VPN Components] > Pre-shared Keys] にある [Template Detail] の各フィールドについて説明します。

表 2-79　[Security] > [VPN Components] > [Pre-shared Keys]

フィールド	説明
IP Address/Host Name	リモート ピアの IP アドレスまたはホスト名を入力します。
Subnet Mask	サブネット マスクを入力します。
Pre-shared Key/ Confirm Pre-shared Key	事前共有キーを入力し、そのキーを再入力して事前共有キーを確認します。

[Security] > [VPN Components] > [RSA-Keys]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Security] > [VPN Components] > [RSA-Keys] にある [Template Detail] の各フィールドについて説明します。

表 2-80　[Security] > [VPN Components] > [RSA-Keys]

フィールド	説明
Label	キー ペアの名前を入力します。
Modulus	キー モジュラス値を入力します。512 ～ 1024 の係数が必要な場合は、64 の倍数となる整数を入力します。1024 よりも大きい値が必要な場合は、1536 または 2048 を入力できます。512 よりも大きい値を入力すると、キー生成に 1 分以上かかる場合があります。 モジュラス値に応じて、キーのサイズが決まります。モジュラスが大きいほどキーの安全性は高くなりますが、大きなモジュラスのキーは生成に要する時間が長くなり、大きなキーほど暗号化/復号化の処理にかかる時間が長くなります。
Type	生成する RSA キーのタイプを選択します。次のオプションがあります。 • general-keys • usages-keys • 暗号化 • シグニチャ
Enable Exportable	エクスポート可能キーとして RSA を生成するには、このフィールドを有効にします。

[Security] > [VPN Components] > [Transform Sets]

トランスフォーム セットは、特定のセキュリティ プロトコルとアルゴリズムを組み合わせたものです。IPSec SA のネゴシエーション中に、ピアは特定のトランスフォーム セットを使用して特定のデータ フローを保護することに合意します。トランスフォーム セットには、特定のセキュリティ プロトコルとそれに対応するアルゴリズムが記述されます。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Security] > [VPN Components] > [Transform Sets] にある [Template Detail] の各フィールドについて説明します。

表 2-81　[Security] > [VPN Components] > [Transform Sets]

フィールド	説明
Name	トランスフォーム セットの名前を入力します。
ESP Encryption	ペイロードの暗号化に使用する ESP 暗号化アルゴリズムを選択します。
ESP Integrity	ペイロードの整合性を確認するために使用する ESP 整合性アルゴリズムを選択します。
AH Integrity	ドロップダウン リストから AH 整合性を選択します。次のオプションがあります。 • MD5（Message Digest 5）（Hash-based Message Authentication Code（HMAC）バリアント）認証アルゴリズムを使用する AH。 • SHA（セキュア ハッシュ アルゴリズム）（HMAC バリアント）認証アルゴリズムを使用する AH。
Compression	Lempel-Ziv-Stac（LZS）アルゴリズムを使用した IP 圧縮を有効または無効にします。
Mode	ドロップダウン リストからモードを選択します。次のオプションがあります。 • [Transport]：データだけを暗号化します。トランスポート モードは、両方のエンドポイントが IPsec をサポートしている場合に使用されます。トランスポート モードでは、認証ヘッダーまたはカプセル化されたセキュリティ ペイロードが元の IP ヘッダーの後に置かれます。これにより、IP ペイロードだけが暗号化されます。この方式を使用すると、暗号化されたパケットに Quality of Service（QoS）制御などのネットワーク サービスを適用できます。 • [Tunnel]：データと IP ヘッダーを暗号化します。トンネル モードはトランスポート モードよりも強力な保護を提供します。IP パケット全体が AH または ESP 内にカプセル化されるため、新しい IP ヘッダーが付加され、データグラム全体を暗号化できます。トンネル モードを使用すると、ルータなどのネットワーク デバイスを複数の VPN ユーザ用の IPsec プロキシとして機能させることができます。トンネル モードは、そのような設定で使用してください。

[Security] > [Zone Based Firewall]

次に、[Configuration] > [Templates] > [Features and Technologies] > [Security] > [Zone Based Firewall] の各フィールドについて説明します。

- [Security] > [Zone Based Firewall] > [Policy Rules]（2-93 ページ）

[Security] > [Zone Based Firewall] > [Policy Rules]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Security] > [Zone Based FireWall] > [Policy Rules] にある [Template Detail] の各フィールドについて説明します。

表 2-82　[Security] > [Zone Based FireWall] > [Policy Rules]

要素	説明
Name	（任意）ポリシー規則の名前を入力します。
Source Zone	インターフェイス ロールのリストから送信元ゾーンを選択します。送信元ゾーンは、トラフィックの起点となるインターフェイスの名前を指定します。
Destination Zone	インターフェイス ロールのリストから宛先ゾーンを選択します。宛先ゾーンは、トラフィックの宛先となるインターフェイスの名前を指定します。

表 2-82　[Security] > [Zone Based FireWall] > [Policy Rules]（続き）

要素	説明
Source	検査対象のデータの送信元 IP アドレスを入力します。有効なパラメータは次のとおりです。 • [Any] • [Other]：[Other] オプションを選択した場合は、IP アドレス、サブネット、およびネットワーク オブジェクトを組み合わせて選択できます。
Destination	検査対象のデータの宛先 IP アドレスを入力します。有効なパラメータは次のとおりです。 • いずれか（Any） • [Other]：[Other] オプションを選択した場合は、IP アドレス、サブネット、およびネットワーク オブジェクトを組み合わせて選択できます。
Service	オブジェクト セレクタから検査対象データのサービスを選択します。有効なパラメータは次のとおりです。 • L3/4 アプリケーション • ACL ベースのアプリケーション：TCP、UDP、ICMP
Action	規則が条件と一致する場合にトラフィック上で実行するアクションを選択します。次の場合に規則が一致します。 • トラフィックの送信元 IP が送信元規則条件と一致。 • トラフィックの宛先 IP が宛先規則条件と一致し、トラフィックの検査対象のサービスがサービス規則条件と一致。 アクションのオプションは次のとおりです。 • [Drop]：ドロップ アクションによって処理されるトラフィックは確認されることなくドロップされます。システムはエンド ホストに通知を送信しません。 • [Drop and Log]：ドロップ アンド ログ アクションで処理されるトラフィックはドロップされ、エンド ホストに syslog 通知が送信されます。 • [Inspect]：検査アクションでは、状態ベースのトラフィック制御が提供され、ルータによって TCP および UDP トラフィックの接続情報またはセッション情報が維持されます。 • [Pass]：このアクションでは、ルータがあるゾーンから別のゾーンにトラフィックを転送します。 • [Pass and Log]：このアクションでは、転送済みトラフィックの syslog 通知の作成中にルータがあるゾーンから別のゾーンにトラフィックを転送します。

[Security] > [DMVPN]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Security] > [DMVPN] にある [Template Detail] の各フィールドについて説明します。

表 2-83　[Security] > [DMVPN]

フィールド		説明
IPsec Information		
IKE Authentication	Authentication Type	[Preshared Keys] オプション ボタンまたは [Digital Certificates] オプション ボタンをオンにします。 • [Preshared Keys]：秘密キーを 2 つのピア間で共有したり、認証フェーズ中に IKE で使用したりできます。 • [Digital Certificates]：IKE キー管理メッセージを署名および暗号化するために、RSA キー ペアが使用される認証方式。証明書によって、2 つのピア間の通信の否認防止が提供されます。つまり、実際に通信が行われたことを証明できます。
	Priority	IKE プロポーザルのプライオリティ値を入力します。このプライオリティ値によって、共通のセキュリティ アソシエーション（SA）の検出試行時に、ネゴシエーションする 2 つのピアを比較することで、IKE プロポーザルの順序が決定します。リモート IPsec ピアが、最初のプライオリティ ポリシーで選択されているパラメータをサポートしていない場合、デバイスは、次に低いプライオリティ番号を持つポリシーで定義されているパラメータの使用を試行します。 有効な値の範囲は、1 ～ 10000 です。値が小さいほど、プライオリティが高くなります。このフィールドをブランクのままにすると、Security Manager によって、まだ割り当てられていない最も小さい値が割り当てられます。値は 1 から始まり、次は 5 となり、その後は 5 ずつ増加します。
	Authentication	ドロップダウン リストから、認証タイプを選択します。

表 2-83　[Security] > [DMVPN]（続き）

フィールド		説明
	D-H Group	Diffie-Hellman（D-H）グループを選択します。D-H グループは、2 つの IPsec ピア間の共有秘密キーを互いに送信することなく取得するために使用されます。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。2 つのピアに、一致する係数グループが設定されている必要があります。次のオプションがあります。 [1]：Diffie-Hellman グループ 1（768 ビット係数）。 [2]：Diffie-Hellman グループ 2（1024 ビット係数）。 [5]：Diffie-Hellman グループ 5（1536 ビット係数。128 ビット キーの保護に推奨されるが、グループ 14 の方がより強力）。AES 暗号化を使用する場合は、このグループ（またはそれ以上）を使用します。ASA では、最上のグループとしてこのグループがサポートされます。
	暗号化	ドロップダウン リストから暗号化アルゴリズムを選択します。この暗号化アルゴリズムを使用してフェーズ 2 ネゴシエーションを保護するためのフェーズ 1 SA を確立します。 [AES-128]：128 ビット キーを使用する AES に従って暗号化を実行します。 [AES-192]：192 ビット キーを使用する AES に従って暗号化を実行します。 [AES-256]：256 ビット キーを使用する AES に従って暗号化を実行します。 [DES]：56 ビット キーを使用する DES に従って暗号化を実行します。 [3DES]：56 ビット キーを使用して暗号化を 3 回実行します。3DES は DES よりもセキュアですが、暗号化と復号化には、より多くの処理を必要とします。ただし、AES に比べるとセキュリティは低くなります。このオプションを使用するには 3DES のライセンスが必要です。
	Hash	IKE プロポーザルで使用されるアルゴリズムを選択します。このハッシュ アルゴリズムによって、メッセージの整合性の確保に使用されるメッセージ ダイジェストが作成されます。次のオプションがあります。 • [SHA (Secure Hash Algorithm)]：160 ビットのダイジェストを生成します。SHA には、総当たり攻撃に対して、MD5 よりも高い耐性が備えられています。 • [MD5 (Message Digest 5)]：128 ビットのダイジェストを生成します。MD5 では、処理時間が SHA よりも少なくなります。

表 2-83　[Security] > [DMVPN]（続き）

フィールド		説明
	IKE Lifetime	IKE ライフタイム値を 60 ～ 86400 の範囲で指定します。デフォルトは 86400 です。このライフタイムを超えると、SA の期限が切れ、2 つのピア間で再ネゴシエーションを行う必要があります。一般的に、一定の限度に達するまで、ライフタイムが短いほど、IKE ネゴシエーションがセキュアになります。ただし、ライフタイムが長いと、今後の IPsec セキュリティ アソシエーションのセットアップが、短いライフタイムの場合よりも迅速に行われます。
Encryption Policy	Name	トランスフォーム セット名を入力します。トランスフォーム セットによって、トンネル上のトラフィックが暗号化されます。
	ESP Encryption	ペイロードの暗号化に使用するアルゴリズムをドロップダウン リストから選択します。次のオプションがあります。 • 128 ビット AES 暗号化アルゴリズムを使用する ESP。 • 192 ビット AES 暗号化アルゴリズムを使用する ESP。 • 256 ビット AES 暗号化アルゴリズムを使用する ESP。 • 168 ビット DES 暗号化アルゴリズム（3DES、トリプル DES とも呼ばれる）を使用する ESP。 • ヌル暗号化アルゴリズム。
	ESP Integrity	ペイロードの整合性の確認に使用する整合性アルゴリズムをドロップダウン リストから選択します。次のオプションがあります。 • MD5（HMAC バリアント）認証アルゴリズムを使用する ESP。 • SHA（HMAC バリアント）認証アルゴリズムを使用する ESP。
	AH Integrity	ドロップダウン リストから [AH integrity] を選択します。次のオプションがあります。 • MD5（Message Digest 5）（Hash-based Message Authentication Code（HMAC）バリアント）認証アルゴリズムを使用する AH。 • SHA（セキュア ハッシュ アルゴリズム）（HMAC バリアント）認証アルゴリズムを使用する AH。
	Compression	ペイロードを圧縮するために IP 圧縮を有効にします。Lempel-Ziv-Stac（LZS）アルゴリズムを使用した IP 圧縮。
	Mode	トラフィックを転送するモードを選択します。

表 2-83　[Security] > [DMVPN]（続き）

フィールド		説明
Topology and Routing Information		
Spoke	—	トポロジ内のスポークとしてルータを設定するには、[Spoke] オプション ボタンをオンにします。
Hub	—	トポロジ内のハブとしてルータを設定するには、[Hub] オプション ボタンをオンにします。 次のルーティング プロトコルのいずれかを選択します。 • [EIGRP]:AS 番号を入力します。 • RIPV2 • Other
Create dynamic connection between Spokes	—	スポーク間に動的な接続を設定するには、[Create Dynamic Connection between Spokes] チェックボックスをオンにします。
Multipoint GRE Interface Information（次のフィールドは、[Operate] > [Device Work Center] の下にだけ表示されます。）		
Select the Tunnel source that connects to internet	—	インターネットに接続する WAN インターフェイスをドロップダウン リストから選択します。
IP Address of this router's GRE Tunnel Interface	—	トンネル インターフェイスの IP アドレスを入力します。
Subnet Mask	—	サブネット マスクを入力します。
NHRP and Tunnel Parameters		
Network ID	—	NHRP のネットワーク ID を入力します。このネットワーク ID は、非ブロードキャスト マルチアクセス（NBMA）ネットワークからの、グローバルに一意の 32 ビット ネットワーク識別子です。範囲は 1 ～ 4294967295 です。
Hold Time	—	（任意）Next Hop Resolution Protocol（NHRP）NBMA アドレスを有効としてアドバタイズする秒数を入力します。デフォルト値は 7200 です。
NHRP Authentication String	—	認証文字列を入力します。
Tunnel Key	—	トンネル キーを入力します。特定のトンネル インターフェイスにキー ID を有効にするために使用します。範囲は 0 ～ 4294967295 です。
Bandwidth	—	帯域幅を入力します。これはオプションのフィールドです。
IP MTU	—	（任意）特定のインターフェイスで送信される IP パケットの MTU サイズを入力します。イーサネットとシリアル インターフェイスに対するデフォルト値は 1500 です。デフォルト値は、メディア タイプによって異なります。

表 2-83　[Security] > [DMVPN]（続き）

フィールド		説明
TCP Maximum Segment Size	—	TCP 最大セグメント サイズを入力します。範囲は 500 ～ 1460 です。
Tunnel Source Interface	—	（任意）物理インターフェイスを入力します。
IPsec Information（次のフィールドは、[Operate] > [Device Work Center] の下にだけ表示されます。）		
Encryption Policy	Name	トランスフォーム セットの名前を入力します。
	ESP Encryption	暗号化アルゴリズムを選択します。ペイロードを暗号化するために使用するアルゴリズムです。
	ESP Integrity	整合性アルゴリズムを選択します。ペイロードの整合性をチェックするために使用するアルゴリズムです。
	AH Integrity	ドロップダウン リストから AH 整合性を選択します。
	Compression	ペイロードの圧縮を有効または無効にするには、適切なオプションを選択します。
	Mode	モードを選択します。トラフィックを転送するためのモードを指定します。
NHS Server		
Cluster Support	Cluster ID	1 つ以上のハブがあるグループを形成するために、クラスタ値を入力します。範囲は 0 ～ 10 です。
	Max Connections	特定のグループまたはクラスタでアクティブにできる接続の最大数を入力します。
	Priority	クラスタ内の特定のハブの優先順位を選択します。ハブ デバイスによってトンネルを形成するスポーク ルータのプライオリティに依存します。
	Next Hop Server	ネクストホップ サーバの IP アドレスを入力します。
IP Address of Hub's physical interface	—	ハブの物理インターフェイスの IP アドレスを入力します。

[Security] > [Easy VPN Remote]

ケーブル モデムや xDSL ルータなど、インターネットへの接続性能が高いブロードバンド アクセスにはさまざまな形式がありますが、多くのアプリケーションでは、高度な認証を実行したり、2 つのエンドポイント間のデータを暗号化したりするなど、VPN 接続に対するセキュリティが必要です。また、2 つのルータ間に VPN 接続を確立するには、複雑な作業が伴う場合がありますし、2 つのルータの VPN パラメータを設定するには普通、ネットワーク管理者間で面倒な調整が必要です。

Cisco Easy VPN のリモート機能を使い、Cisco Unity Client プロトコルを実装することで、ほとんどの VPN パラメータが Cisco IOS Easy VPN サーバで定義できるようになるため、こうした面倒な作業が大幅に軽減されます。サーバには、Cisco VPN 3000 シリーズ コンセントレータや Cisco PIX ファイアウォールなどの専用 VPN デバイスを使用できるほか、Cisco Unity Client プロトコルをサポートする Cisco IOS ルータも使用できます。

Cisco Easy VPN サーバを設定すると、最小設定の VPN 接続がシスコ デバイス上に作成されます。Easy VPN Remote による VPN トンネル接続が開始すると、Cisco Easy VPN サーバでは、IPsec ポリシーが Easy VPN Remote にプッシュされ、それに対応する VPN トンネル接続が構成されます。

Easy VPN Client テンプレートを作成する前に、同一アドレッシング ACL、対象トラフィック ACL、保護サブネット ACL などの必要な ACL を ACL テンプレートを使用して作成します。詳細については、*『Cisco Prime Infrastructure 3.0 User Guide』*を参照してください。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Security] > [Easy VPN Remote] にある [Template Detail] の各フィールドについて説明します。

表 2-84　[Security] > [Easy VPN Remote]

フィールド		説明
Easy VPN Remote Profile Name and Interface Configuration		
Profile Name	—	プロファイル名を入力します。
Interface and Server Association	Inside Interfaces	これらは、Easy VPN 接続に組み込まれているインターフェイスです。これらのインターフェイスに接続されたすべてのホストまたはサブネットが VPN に含まれます。
	Outside Interfaces	Easy VPN サーバまたはコンセントレータに接続する WAN インターフェイス。
	Virtual Template Number	この番号によって、ルーティング可能なインターフェイスを指定し、選択したトラフィックをさまざまな Easy VPN コンセントレータへ送信してインターネットへ送信します。
	Easy VPN Server	Easy VPN サーバ アドレスを入力します。最大 10 個の IPv4 サーバ アドレスまたはサーバ ホスト名を追加できます。
	Idle Time	サーバのアイドル時間を秒単位で入力します。範囲は 60 ～ 86400 です。デフォルト値は 60 です。

表 2-84　[Security] > [Easy VPN Remote]（続き）

フィールド		説明
Each VPN Remote Connection Settings		
Mode of Operation	クライアント	ルータの内部ネットワーク上の PC やその他のデバイスでプライベート IP アドレスを持つプライベート ネットワークを形成する場合は、[Client] を選択します。トラフィックのルーティングにはネットワーク アドレス変換（NAT）とポート アドレス変換（PAT）が使用されます。LAN 外部のデバイスは、LAN 上のデバイスを ping したり、それらのデバイスに直接到達したりできなくなります。
	Network Extension	デバイスを内部インターフェイスに接続しており、ルーティング可能で、宛先ネットワークが到達可能な IP アドレスを取得する場合は、[Network Extension] を選択します。接続の両端のデバイスは、一体となって 1 つの論理ネットワークを形成します。PAT は自動的に無効になっており、接続の両端にある PC やホストが相互にダイレクト アクセスできるようになっています。
	Network Extension Plus	モード設定により IP アドレスを要求し、利用可能なループバック インターフェイスに自動的に割り当てるには、[Network Extension Plus] モードを選択します。この IP アドレスの IPsec SAは、Easy VPN Remote により自動的に作成されます。この IP アドレスを使用してルータに接続し、リモート管理およびトラブルシューティング（ping、Telnet、およびセキュア シェル）を行うことができます。 **注**　ルータが Easy VPN Remote Phase 4 以降をサポートする Cisco IOS イメージを実行していない場合は、Network Extension Plus モードを設定できません。
Protected Subnets ACL	—	指定された内部インターフェイスの直接的な部分ではないサブネットの ACL を入力します。
Connection Method	Auto	Easy VPN 設定がルータ設定ファイルに配信される場合に VPN トンネルを自動的に確立するには、[Auto] を選択します。ただし、トンネルを手動で制御できなくなります。
	Manual	VPN トンネルがいつ確立され、いつ終了するかを制御する場合は、[Manual] を選択します。
	Interesting Traffic	特定のトラフィックが検知されたときにのみトンネルを確立する場合は、[Interesting Traffic] を選択します。このトラフィックは、対象トラフィック ACL で特定されます。
EasyVPN Remote Authentication Mechanisms		
Primary Authentication	—	デバイス認証方式を選択します。[Pre-shared Key] または [Digital Certificate] を選択できます。

表 2-84　[Security] > [Easy VPN Remote]（続き）

フィールド		説明
Pre Shared Key Configuration	Group Name	IPsec グループ名を入力します。このグループ名は、VPN コンセントレータまたはサーバで定義されているグループ名と一致する必要があります。この情報は、ネットワーク管理者から取得してください。
	Enable Encrypted Password	パスワードを暗号化するには [Enable Encrypted Password] チェックボックスをオンにします。
	Pre Shared Key	[Preshared Keys] をオンにすると、秘密キーを 2 つのピア間で共有したり、認証フェーズ中に IKE で使用したりできます。
	Confirm Pre Shared Key	事前共有キーを再入力し、そのキーを確認します。
Digital Certificate	—	IKE キー管理メッセージを署名および暗号化するために RSA キー ペアを使用する認証方式。証明書によって、2 つのピア間の通信の否認防止が提供されます。つまり、実際に通信が行われたことを証明できます。
Extended Authentication		
Enable XAuth	—	Cisco IOSデバイスのデフォルトでは、[Enable XAuth] は有効になっています。
Use Web Authentication	—	Web 認証方式を使用するには、[Use Web Authentication] オプション ボタンをオンにします。HTTP 認証を使用するには、[Use HTTP Authorization for each client behind the Easy VPN Remote] チェックボックスをオンにします。
Save Credentials	—	[Save Credentials] オプション ボタンをオンにし、ユーザ名とパスワードを指定します。パスワードを確認するため、そのパスワードを再入力します。
Prompt for Credential	—	[Prompt for Credentials] オプション ボタンをオンにし、クレデンシャルを指定します。
EasyVPN Remote Firewall Settings		
Enable EasyVPN through Firewall	—	ファイアウォール設定を有効にするには、[EasyVPN through Firewall] チェックボックスをオンにします。
cTCP Port Number	—	Cisco Tunneling Control Protocol（cTCP）ポート番号を入力します。この番号は、EZVPN サーバの cTCP ポート番号と一致する必要があります。有効な範囲は 1 ～ 65535 です。デフォルト値は 10000 です。
NAT/Firewall Keepalive	—	ファイアウォールのキープアライブ時間を秒単位で入力します。範囲は 5 ～ 3600 です。デフォルト値は 5 です。

[Security] > [Easy VPN Server]

Easy VPN サーバ 機能により、Cisco VPN Client Release 3.*x* 以降、および Cisco VPN ハードウェア クライアント（Cisco Integrated Services ルータやシスコ アプリケーション固有のルータなど）がサーバのサポート対象となりました。IP Security（IPsec）を使用して、集中管理された IPsec ポリシーがサーバによってクライアント デバイスにプッシュされ、エンド ユーザの設定を最小限に抑えることができます。

Easy VPN サーバの設定に、動的な仮想トンネル インターフェイスやダイナミック暗号マップ方式を使用できます。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Security] > [Easy VPN Server] にある [Template Detail] の各フィールドについて説明します。

表 2-85　[Security] > [Easy VPN Server]

フィールド		説明
Validation Criteria		
Device Type	—	[Routers] を選択します。
Interface Configuration Methods		
Outside Interface	—	WAN リンクに接続するインターフェイス名を入力します。
Configure Dynamic Virtual Tunnel Interface	—	[IPsec Profile] テンプレート（[Security] > [VPN Components] > [IPSec Profile]（2-91 ページ）を参照）で作成した仮想テンプレート番号と IPsec プロファイル名を入力します。または、デバイスに存在している IPsec プロファイルの名前も入力できます。デバイスに存在している IPsec プロファイルは、デバイス ビューに表示されます。
Configure Dynamic Crypto Map	—	[Transform Set] テンプレート（[Security] > [VPN Components] > [Transform Sets]（2-92 ページ）を参照）で作成した暗号マップとトランスフォーム セット名を入力します。または、デバイスに存在しているトランスフォーム セットの名前も入力できます。デバイスに存在しているトランスフォーム セットは、デバイス ビューに表示されます。
ISAKMP Settings		
Client Configuration Address Type	—	ドロップダウンリストからクライアント設定のアドレス タイプを選択します。
Enable Dead Peer Detection	—	デッド ピア検出（DPD）メッセージを Easy VPN クライアントに送信するように、デバイスを有効にします。クライアントが DPD メッセージに応答しない場合は、接続は終了されます。
Keep Alive Interval	—	DPDメッセージ間隔を [Keepalive Interval] フィールドに秒単位で指定します。範囲は 10 ～ 3600 です。
Retry Interval	—	DPD メッセージが失敗した場合の再試行間隔を秒単位で指定します。範囲は 2 ～ 60 です。
AAA Group/User Policy		
AAA Group Method List	—	CLI テンプレートで作成したものと同じ AAA グループ メソッド リストのプロファイル名を入力します。
AAA User Method List	—	CLI テンプレートで作成したものと同じ AAA ユーザ メソッド リストのプロファイル名を入力します。
Enable PKI download	—	AAA サーバからユーザ属性を取得し、モード設定を使用してリモート デバイスにプッシュするには、[Enable PKI download] チェックボックスをオンにします。属性を取得する際に使用するユーザ名は、リモート デバイスの証明書から取得されます。
VPN groups	—	ルータ内にローカルに存在しないものの、そのアイデンティティは ISAKMP プロファイルと一致する必要がある ISAKMP グループを指定します。

表 2-85　[Security] > [Easy VPN Server]（続き）

フィールド		説明
EasyVPN Group Configuration		
General		
General	[Group Name]	Easy VPN グループ名を入力します。
	Enable Encrypted Key	暗号化された事前共有キーを指定できるようにするには、[Enable Encrypted Key] チェックボックスをオンにします。
	Pre-Shared Key	[Preshared Keys] を使用すると、秘密キーを 2 つのピア間で共有したり、認証フェーズ中に IKE で使用したりできます。
	Confirm Pre-Shared Key	事前共有キーを再入力し、そのキーを確認します。
Address Pool Configuration	Assign IP Address to Remote Clients	クライアントへ内部 IP アドレスを割り当てるための新しい IP アドレス プールを作成するには、[Assign IP Address to Remote Clients] チェックボックスをオンにします。
	Starting IP Address	範囲の開始 IP アドレス（例:1.1.1.1）を入力します。
	Ending IP Address	範囲の終了 IP アドレス（例:1.1.1.1 ～ 1.1.254.1）を入力します。
	Subnet Mask	ローカル接続の接続先クライアントが使用するサブネット マスクを入力します。
	Max Connections Allowed	設定できる接続の最大数を入力します。値の範囲は 1 ～ 5000 です。
XAuth Options	Enable XAuth	拡張認証方式を有効にするには、[Enable XAuth] チェックボックスをオンにします。
	XAuth Banner	サーバが Easy VPN Remote にプッシュするバナーを入力します。
	Max Logins allowed per user	ユーザごとに許可する最大ログイン数。値の範囲は 1 ～ 10 です。
	Enable group lock for XAuth	XAuth 時に追加の認証確認を実行するには、[Enable group lock for XAuth] チェックボックスをオンにします。XAuth 時に入力したグループ名は、事前共有キー デバイス認証用に送信したグループ名でサーバによって比較されます。それらのグループ名が一致しない場合は、サーバにより接続が拒否されます。
	Save XAuth password on router	後続のサーバへの接続時の IKE モード設定中にポリシーを受け取った後、XAuth クレデンシャルを入力するように求められた際、クライアントはパスワードをローカルに保存できます。
DNS & WINS		
Domain Name	—	グループが属する DNS ドメインの名前を入力します。
Configure DNS Servers	—	グループのプライマリおよびセカンダリ DNS サーバを指定するには、[Configure DNS Servers] チェックボックスをオンにします。
Primary DNS Server	—	プライマリ DNS サーバの IP アドレスを入力します。
Secondary DNS Server	—	セカンダリ DNS サーバの IP アドレスを入力します。
Configure WINS Server	—	グループのプライマリおよびセカンダリ DNS サーバを指定するには、[Configure WINS Server] チェックボックスをオンにします。
Primary WINS Server	—	プライマリ WINS サーバの IP アドレスを入力します。

表 2-85　[Security] > [Easy VPN Server]（続き）

フィールド		説明
Secondary WINS Server	—	セカンダリ WINS サーバの IP アドレスを入力します。
Split Tunneling		
Split Tunnel ACL	—	スプリット トンネリング用の保護サブネットを表す ACL の名前を入力します。
Split DNS Configuration	—	プラベート ネットワークに対してトンネリングまたは解決する必要のあるドメイン名を入力します。
Settings		
Configuration Push	URL	リモート デバイスがサーバから設定を取得する際に使用する URL を入力します。この URL は、設定済みファイルの完全パスを指定する非ヌル終端 ASCII 文字列である必要があります。
	Version	設定のバージョンを入力します。範囲は 1 ～ 32767 です。
Backup Configuration	Backup Gateways	バックアップ ゲートウェイを割り当てて、クライアント デバイスにバックアップ ゲートウェイのリストをプッシュします。これまでのゲートウェイが失敗した場合に、これらのゲートウェイが使用されます。
Access Settings	Include local LAN	クライアントと同時にローカル サブネットワークにアクセスするために非スプリット トンネリング接続を許可するには、[Include local LAN] チェックボックスをオンにします。
	Enable perfect forward secrecy	IPsec SA に Perfect Forward Secrecy が必要かどうかについてクライアントに通知するには、[Enable perfect forward secrecy] チェックボックスをオンにします。
Firewall and Proxy Settings	Enable Firewall Are-U-There	Are-U-There ファイアウォールを有効にするには、[Enable Firewall Are-U-There] チェックボックスをオンにします。
	Browse Proxy Settings	Easy VPN ブラウザ プロキシ テンプレートが設定したブラウザ プロキシ プロファイルを入力します。
Firewall Settings		
Enable cTCP	—	Easy VPN の cTCP カプセル化を設定するには、[Enable cTCP] チェックボックスをオンにします。最大 10 個のポート番号を設定できます。
cTCP Port Number(s)	—	cTCP のポート番号を入力します。
cTCP Keep Alive	—	cTCP キープ アライブ時間を秒単位で入力します。範囲は 5 ～ 3600 です。

[Security] > [Easy VPN Server Proxy Setting]

Easy VPN サーバのプロキシ設定機能では、Easy VPN リモートと Easy VPN クライアントに対して Easy VPN サーバがプッシュするブラウザ プロキシ設定を指定できます。Easy VPN サーバのプロキシ設定機能を使用すると、Cisco IOS VPN クライアントを使用して社内ネットワークに接続する際に Web ブラウザのプロキシ設定を手動で変更する必要はありません。また、ネットワークから切断する際にプロキシ設定を手動で元に戻す必要もありません。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Security] > [Easy VPN Server Proxy Setting] にある [Template Detail] の各フィールドについて説明します。

表 2-86　[Security] > [Easy VPN Server Proxy Setting]

フィールド	説明
Browser Proxy Name	ブラウザのプロキシ設定のプロファイル名を入力します。
Proxy Server Settings Used by Client Browser	• このグループのクライアントにプロキシ サーバを使用させない場合は、[No Proxy Server] オプションを選択します。 • このグループのクライアントが VPN トンネルで使用する際にそれらのクライアントにプロキシ サーバを自動的に検出するには、[Automatically Detect Proxy Settings] オプションを選択します。 • このグループのクライアントにプロキシ サーバを手動で設定するには、[Manual Configuration] オプションを選択します。
IP Address of Proxy Server	プロキシ サーバの IP アドレスを入力します。
Port	プロキシ サーバのポート番号を入力します。
Do not Use Proxy Server for Accessing the Following Hosts	プロキシ サーバを使用しないホストのアドレスを入力します。
Bypass Proxy Serve for Local Addresses	クライアントがローカル(LAN)アドレスにプロキシ サーバを使用しないようにする場合は、このチェックボックスをオンにします。

[Security] > [GETVPN-GroupMember]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Security] > [GET VPN Group Member] にある [Template Detail] の各フィールドについて説明します。

表 2-87　[Security] > [GET VPN Group Member]

フィールド		説明
グループ情報		
Group ID	—	グループ ID を入力します。これは、GETVPN グループ メンバの一意の識別子です。数値または IP アドレスを指定できます。
Group Name	—	GETVPN グループ メンバのグループ名を入力します。

表 2-87　[Security] > [GET VPN Group Member]（続き）

フィールド		説明
IKE Authentication Policy	—	この固定されたフィールドと関連付けられたポップアップ ダイアログ ボックスを使用して、この GETVPN グループ メンバの認証タイプとポリシーを指定します。
	Pre-Shared Key	IKE 認証タイプとして事前共有キーを選択するには、このオプション ボタンをオンにします。このオプション ボタンをオンにした場合は、このボタンのすぐ下にある [Pre-Shared Key] フィールドにキーを入力する必要があります。
	Confirm Pre-Shared Key	事前共有キーを再入力して確認します。このフィールドは、認証タイプとして事前共有キーを選択した場合にのみ表示されます。
	Digital Certificate	IKE 認証タイプとしてデジタル証明書を選択するには、このオプション ボタンをオンにします。この認証タイプを選択した場合は、ルータには、そのルータ自体を認証するために認証局によって発行されたデジタル証明書が必要です。
	Priority	値 1 ～ 10000 を入力し、認証ポリシーのネゴシエーション優先順位を設定します（最も高い優先度は 1）。このプライオリティ値によって、共通の SA の検出試行時に、ネゴシエーションする 2 つのピアを比較することで、IKE プロポーザルの順序が決定します。リモート IPsec ピアが、最初のプライオリティ ポリシーで選択されているパラメータをサポートしていない場合、デバイスは、次に低いプライオリティ番号を持つポリシーで定義されているパラメータの使用を試行します。
	Authentication	認証ポリシーの認証タイプをリストから選択します。
	D-H Group	認証ポリシーの D-H グループをリストから選択します。
	暗号化	認証ポリシーの暗号化タイプをリストから選択します。
	Hash	認証ポリシーのハッシュ タイプをリストから選択します。
	IKE Lifetime	SA ライフタイムを秒単位で入力します。このライフタイムを超えると、SA の期限が切れ、2 つのピア間で再ネゴシエーションを行う必要があります。一般に、ライフタイムが短いほど、IKE ネゴシエーションがセキュアになります。
WAN Interface	—	GETVPN グループ メンバの WAN インターフェイス登録情報を入力します。
Traffic Details		
Local Exception Policy ACL	—	GETVPN グループ メンバがクリア テキストで送信する必要があるトラフィックを指定するローカル例外ポリシー ACL を入力します。
Fail Close ACL	—	GETVPN 暗号化が失敗したときに許可する必要があるトラフィックを指定するフェール クローズ ACL を入力します。フェール クローズ ACL 機能を設定した場合、グループ メンバ経由で通過するすべてのトラフィックは、グループ メンバが正常に登録されるまでドロップされます。グループ メンバが正常に登録され、SA がダウンロードされた後に、この機能は自動的に無効になります。

表 2-87　[Security] > [GET VPN Group Member]（続き）

フィールド		説明
Key Servers		
Primary Key Server	—	プライマリ暗号キー サーバの IP アドレスまたはホスト名を入力します。プライマリ キー サーバは、グループ ポリシーを作成してすべてのグループ メンバに配布する処理、およびセカンダリ キー サーバと定期的に同期する処理を担当します。
Secondary Key Servers	—	一連のセカンダリ キー サーバを指定するには、この編集テーブルを使用します。編集テーブルの最上部に優先度が最も高いサーバが来るように、優先度順にサーバを入力します。プライマリ キー サーバがダウンしていたり、アクセスできない状態にある間、優先度が一番高いアクセス可能なセカンダリ キー サーバがプライマリ キー サーバとして機能するように選択されます。
Enable Passive SA	—	グループ メンバでパッシブ SA モードを有効にするには、[Enable Passive SA] チェックボックスをオンにします。

[Security] > [GETVPN-KeyServer]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Security] > [GET VPN Key Server] にある [Template Detail] の各フィールドについて説明します。

表 2-88　[Security] > [GET VPN Key Server]

フィールド	説明
Template Detail	
[Group Name]	GETVPN グループ メンバ テンプレートのグループ名を入力します。
Group ID	GETVPN グループ メンバの一意の ID を入力します。数値または IP アドレスを指定できます。number の範囲は 0 ～ 2147483647 です。
IKE Authentication Policy	
Authorization Type	[Preshared Keys] オプション ボタンまたは [Digital Certificates] オプション ボタンをクリックします。 • [Preshared Keys]：秘密キーを 2 つのピア間で共有したり、認証フェーズ中に IKE で使用したりできます。 • [Digital Certificates]：IKE キー管理メッセージを署名および暗号化するために、RSA キー ペアが使用される認証方式。証明書によって、2 つのピア間の通信の否認防止が提供されます。つまり、実際に通信が行われたことを証明できます。
Priority	IKE プロポーザルのプライオリティ値。このプライオリティ値によって、共通の SA の検出試行時に、ネゴシエーションする 2 つのピアを比較することで、IKE プロポーザルの順序が決定します。リモート IPsec ピアが、最初のプライオリティ ポリシーで選択されているパラメータをサポートしていない場合、デバイスは、次に低いプライオリティ番号を持つポリシーで定義されているパラメータの使用を試行します。 有効な値の範囲は、1 ～ 10000 です。値が小さいほど、プライオリティが高くなります。

表 2-88　[Security] > [GET VPN Key Server]（続き）

フィールド	説明
暗号化	ドロップダウン リストから暗号化アルゴリズムを選択します。この暗号化アルゴリズムを使用してフェーズ 2 ネゴシエーションを保護するためのフェーズ 1 SA を確立します。 • [AES-128]：128 ビット キーを使用する AES に従って暗号化を実行します。 • [AES-192]：192 ビット キーを使用する AES に従って暗号化を実行します。 • [AES-256]：256 ビット キーを使用する AES に従って暗号化を実行します。 • [DES]：56 ビット キーを使用する DES に従って暗号化を実行します。 • [3DES]：56 ビット キーを使用して暗号化を 3 回実行します。3DES は DES よりもセキュアですが、暗号化と復号化には、より多くの処理を必要とします。AES に比べるとセキュリティは低くなります。このオプションを使用するには 3DES のライセンスが必要です。
Hash	IKE プロポーザルで使用されるハッシュ アルゴリズム。このアルゴリズムによって、メッセージの整合性の確保に使用されるメッセージ ダイジェストが作成されます。次のオプションがあります。 • [SHA (Secure Hash Algorithm)]：160 ビットのダイジェストを生成します。SHA には、総当たり攻撃に対して、MD5 よりも高い耐性が備えられています。 • [MD5 (Message Digest 5)]：128 ビットのダイジェストを生成します。MD5 では、処理時間が SHA よりも少なくなります。
Diffie-Hellman Group	Diffie-Hellman グループは、2 つの IPsec ピア間の共有秘密キーを互いに送信することなく取得するために使用されます。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。2 つのピアに、一致する係数グループが設定されている必要があります。次のオプションがあります。 • [1]：Diffie-Hellman グループ 1（768 ビット係数）。 • [2]：Diffie-Hellman グループ 2（1024 ビット係数）。 • [5]：Diffie-Hellman グループ 5（1536 ビット係数。128 ビット キーの保護に推奨されるが、グループ 14 の方がより強力）。AES 暗号化を使用する場合は、このグループ（またはそれ以上）を使用します。ASA では、最上のグループとしてこのグループがサポートされます。
Lifetime	SA のライフタイム（秒数）。このライフタイムを超えると、SA の期限が切れ、2 つのピア間で再ネゴシエーションを行う必要があります。一般的に、一定の限度に達するまで、ライフタイムが短いほど、IKE ネゴシエーションがセキュアになります。ただし、ライフタイムが長いと、今後の IPsec セキュリティ アソシエーションのセットアップが、短いライフタイムの場合よりも迅速に行われます。 60 ～ 2147483647 の値を指定できます。デフォルトは 86400 です。
Registration Interface	暗号マップを関連付ける必要があるインターフェイスの名前を入力します。
Traffic Details	
Local Exception ACL	暗号化から除外する必要があるトラフィックの ACL を選択します。

表 2-88　[Security] > [GET VPN Key Server]（続き）

フィールド	説明
Fail Close ACL	グループ メンバがキー サーバに登録されるまで、クリア テキストで送信する必要があるトラフィックの ACL を選択します。フェール クローズ機能を設定した場合、グループ メンバ経由で通過するすべてのトラフィックは、グループ メンバが正常に登録されるまでドロップされます。グループ メンバが正常に登録され、SA がダウンロードされた後に、この機能は自動的に無効になります。
Key Server Information	
Primary Key Server	クライアントを接続するプライマリ キー サーバの IP アドレスを指定します。プライマリ キー サーバは、グループ ポリシーを作成してすべてのグループ メンバに配布する処理、およびセカンダリ キー サーバと定期的に同期する処理を担当します。プライオリティが最も高いサーバが、プライマリ キー サーバとして選択されます。
Secondary Key Server	プライマリ キー サーバの登録に失敗した場合に、グループ メンバがフォールバックするセカンダリ キー サーバの IP アドレスを指定します。すべてのセカンダリ キー サーバのリストから使用可能な任意のキー サーバに登録するようにグループ メンバを設定できます。グループ メンバの設定によって、登録順序が決定されます。最初に定義されたキー サーバに対して接続が試みられ、その後、定義された順番でキー サーバへの接続が試みられます。グループ メンバに対して最大 8 台のキー サーバを割り当てることができます。
Migration	
Enable Passive SA	グループ メンバでパッシブ SA モードを有効にするには、このオプションを使用します。パッシブ SA モードでは、キー サーバの受信専用 SA オプションが上書きされ、すべての発信トラフィックが暗号化されます。
[Group Name]	GETVPN グループ メンバ テンプレートのグループ名を入力します。

[Security] > [ScanSafe]

Cisco Scansafe による Cisco ISR Web セキュリティは、クラウドベースのサービスとしてのセキュリティ（SaaS）で、HTTP や HTTPs のトラフィックのコンテンツをスキャンできます。Cisco ScanSafe による Cisco ISR Web セキュリティをルータと統合すると、選択した HTTP や HTTPS のトラフィックが ScanSafe クラウドにリダイレクトされ、コンテンツのスキャンとマルウェア検出が行われます。

Web トラフィックを Cisco ScanSafe による Cisco ISR Web セキュリティにリダイレクトするように Cisco ScanSafe による Cisco ISR Web セキュリティを設定すると、ISR は IP アドレスとポートに基づいて HTTP および HTTPS のトラフィックを ScanSafe のプロキシ サーバに透過的にリダイレクトします。Cisco ScanSafe による Cisco ISR Web セキュリティによるスキャンが実行されることなく、最初に要求した Web サーバに Web トラフィックを直接リレーするように ISR を設定できます。

トラフィックのホワイトリスト

承認された Web トラフィックが Cisco ScanSafe による Cisco ISR Web セキュリティにリダイレクトされ、スキャンが行われないように ISR を設定できます。このスキャンをバイパスすると、ISR は、Cisco ScanSafe による Cisco ISR Web セキュリティに問い合わせることなく最初に要求した Web サーバからコンテンツを直接取得します。Web サーバから応答を受け取ると、データをクライアントに送信します。これをトラフィックの *ホワイトリスト*といいます。

ScanSafe の詳細については、
http://www.cisco.com/en/US/docs/security/web_security/ISR_SS/ISR_ScanSafe_SolutionGuide.pdf を参照してください。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Security] > [ScanSafe] にある [Template Detail] の各フィールドについて説明します。

表 2-89　[Security] > [ScanSafe]

フィールド	説明
Server Information	
Primary Server	プライマリ ScanSafe サーバの IPv4 アドレスまたはホスト名を入力します。
HTTP Port	HTTP 要求がプライマリ サーバにリダイレクトされる HTTP ポートを指定します。デフォルトでは、ScanSafe は HTTP トラフィックについてはポート 80 を使用します。ただし、要求タイプごとに異なるポートを使用するよう選択できます。
HTTPS Port	HTTPS 要求をプライマリ サーバにリダイレクトする HTTPS ポートを指定します。デフォルトでは、ScanSafe は HTTPS トラフィックについてはポート 443 を使用します。ただし、要求タイプごとに異なるポートを使用するよう選択できます。
Secondary Server	セカンダリ ScanSafe サーバの IPv4 アドレスまたはホスト名を入力します。
HTTP Port (secondary)	HTTP 要求がセカンダリ サーバにリダイレクトされる HTTP ポートを指定します。デフォルトでは、ScanSafe は HTTP トラフィックについてはポート 80 を使用します。
HTTPS Port	HTTPS 要求がセカンダリ サーバにリダイレクトされる HTTPS ポートを指定します。デフォルトでは、ScanSafe は HTTPS トラフィックについてはポート 443 を使用します。
Scansafe License	要求を開始した組織を示すために ISR が ScanSafe プロキシ サーバに送信するライセンス キーを指定します。ライセンスは 16 バイトの 16 進キーです。
Encrypt License Info	ライセンス情報を暗号化するには、[Encrypt License Info] チェックボックスをオンにします。
Server Timeout	プライマリ ScanSafe サーバのタイムアウトを秒単位で指定します。ISR は指定されたタイムアウト期間を待機してから、ScanSafe プロキシ サーバをポーリングし、利用可能かどうかを確認します。
Session Timeout	プライマリ ScanSafe セッションのアイドル タイムアウトを秒単位で指定します。プライマリ サーバに障害が発生した場合、ISR はセカンダリ サーバをアクティブな ScanSafe プロキシ サーバとして使用します。連続する 3 回のタイムアウト期間にアクティブである場合、ISR は自動的にプライマリ サーバにフォール バックします。
Source Interface	ScanSafe が有効になっている送信元の IPv4 アドレスまたはインターフェイス名を指定します。
Router behavior when ScanSafe server fail to respond	着信トラフィックが設定された ScanSafe プロキシ サーバに到達できない場合に、ISR がそのトラフィックをどのように処理するかを指定します。オプションはすべてのトラフィックをドロップする [Drop all traffic] か、すべてのトラフィックを許可する [Allow all traffic] です。デフォルトは [Drop all traffic] です。
User Information	
Global User	ルータの入力インターフェイスに Web 認証（webauth）が設定されていない場合は、グローバル ユーザを入力します。
Global User Group	ルータの出力インターフェイスに Web 認証（webauth）が設定されていない場合は、グローバル ユーザ グループを入力します。
User Group Inclusion & Exclusion Info	2 つの編集テーブルを使用して、ScanSafe タワーとのやり取り時に含める、または除外するユーザ グループ情報を指定します。ユーザ グループ情報は、ルータの入力および出力インターフェイスに Web 認証（webauth）が設定する場合にのみ使用されます。
Notify Whitelist Info to ScanSafe Tower	ScanSafe タワーにホワイトリスト情報を送信し、送信する Safe URL、Safe ユーザ エージェント、Safe ACL 情報を指定するにはこのオプションを選択します。

[CLI Templates] フィールドの説明

次に、システム CLI テンプレートで使用されているフィールドについて説明します。

802.1X Change of Authorization-IOS

スイッチの動的認証を行うための RADIUS クライアント設定をサポートするには、このオプションを使用します。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Templates] > [CLI Templates] > [System Templates - CLI] > [802.1X Change of Authorization-IOS] にある [Template Detail] の各フィールドについて説明します。

表 2-90　[CLI Templates] > [System Templates - CLI] > [802.1X Change of Authorization-IOS]

フィールド	説明
Form View	
RADIUS client IP Address or Host Name	DNShost 名または RADIUS サーバ ホストの IP アドレス
Type of authorization the device uses for RADIUS clients	RADIUS クライアントにデバイスが使用する必要がある認証のタイプ([any]、[all]、または [session key])を指定します。クライアントは、認証用に設定された属性と一致していなければなりません。
RADIUS Key shared between the device and RADIUS clients	RADIUS サーバの認証および暗号キーを指定します。 キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用できます。キーにスペースを使用する場合は、引用符自体がキーの一部でない限り、そのキーを引用符で囲まないでください。
Port on which the device listens for RADIUS requests	デバイスが RADIUS の要求をリッスンするポート番号を指定します。 ポート番号の範囲は 0 ～ 65535 です。デフォルト値は 1700 です。

Access Layer-IOS

プラットフォーム、LAN スイッチのユニバーサル設定、アクセス スイッチのグローバル設定、クライアント接続を設定し、デバイスをディストリビューション ルータまたは WAN ルータに接続するには、このオプションを使用します。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Templates] > [CLI Templates] > [System Templates - CLI] > [Access Layer-IOS] にある [Template Detail] の各フィールドについて説明します。

表 2-91　[CLI Templates] > [System Templates - CLI] > [Access Layer-IOS]

フィールド	説明
[Form View] タブ	
Device Type	選択したデバイス タイプにのみテンプレートを展開します。 **注**　展開上の問題を避けるため、このフィールドは編集しないでください。
Device OID	選択したデバイス OID にのみテンプレートを展開します。 **注**　展開上の問題を避けるため、このフィールドは編集しないでください。
Switch Number	Catalyst 2960-S および 3750-X プラットフォームのスイッチ番号を入力します。
LAN Switch Universal Configuration	
Host name	設定するデバイスのホスト名を入力します。
IP Domain-name	非完全修飾ホスト名(ドット付き 10 進表記ドメイン名のない名前)を完成させるために Cisco IOS ソフトウェアが使用する、デフォルトのドメイン名を入力します。ドメイン名を未修飾の名前から区切るために使用される最初のピリオドは入れないでください。
SNMP-server community RO	Simple Network Management Protocol(SNMP)へのアクセスを許可するコミュニティ アクセス文字列を設定する、SNMP サーバ コミュニティの読み取り専用アクセス(RO)を入力します。

表 2-91　[CLI Templates] > [System Templates - CLI] > [Access Layer-IOS]（続き）

フィールド	説明
SNMP-server community RW	Simple Network Management Protocol（SNMP）へのアクセスを許可するコミュニティ アクセス文字列を設定するには、SNMP サーバ コミュニティの読み取り/書き込みアクセス権（RW）を入力します。
Enable Secret Password	自動的に暗号化を実行するには、[Enable Secret Password] コマンドを入力します。
Username Admin Password	ユーザ名管理パスワードを入力します。
IP Address of Tacacs Server	TACACS サーバの IP アドレスを入力します。
TACACS Key	スイッチを TACACS サーバに対して認証するには、TACACS 秘密キーを入力します。
NTP Server IP Address	アプリケーションやその他のデスクトップ プロセスのクロックの同期を保持するために、NTP サーバの IP アドレスを入力します。
Time Zone	新しい夏時間（DST）の変更に適合するには、タイム ゾーンを入力します。
Hours offset from UTC	協定世界時間（UTC）から遅れている、または進んでいる時間数を選択します。
Minutes offset from UTC	協定世界時間（UTC）から遅れている、または進んでいる分数を入力します。
Summer Time zone	夏時間を入力します。
Access Switch Global Settings and Client Connectivity	
Voice VLAN	IP 電話からの IP 音声トラフィックを搬送するアクセス ポートを有効にするには、音声 VLAN を入力します。
Data VLAN	ユーザ生成トラフィックのみを搬送するには、データ VLAN を入力します。
Configure Access Switch Global Settings	
Management VLAN	telnet、SSH、SNMP、syslog などのプロトコルを使用してリモートの場所からスイッチを管理するための管理 VLAN を入力します。
Management IP Address	ネットワークで使用される IP アドレス空間を検出、モニタ、監査、および管理するための管理 IP アドレスを入力します。
Management Subnet Mask	管理サブネット マスクを入力します。
Default Router IP Address	デフォルト ルータの IP アドレスを入力します。
Other Settings	
Interface Type to Configure Client Connectivity	ドロップダウンリストからインターフェイス タイプを選択します。
Start Interface Number	開始インターフェイス番号を入力します。例えば、Gigabit Ethernet の場合は 0/1、PortChannel の場合は 1 などです。
End Interface Number	終了インターフェイス番号を入力します。例えば、2 などです。
Connect to Distribution or WAN Router	ドロップダウン リストから必要なオプションを選択します。
Channel Group Number	EtherChannel インターフェイスを EtherChannel グループに割り当てて設定するには、チャネル グループ番号を入力します。
Interface Type for Connect to Distribution or WAN Router	ドロップダウンリストからインターフェイス タイプを選択します。
Start Interface Number	開始インターフェイス番号を入力します。例えば、Gigabit Ethernet の場合は 0/1、PortChannel の場合は 1 などです。

表 2-91　[CLI Templates] > [System Templates - CLI] > [Access Layer-IOS]（続き）

フィールド	説明
End Interface Number	終了インターフェイス番号を入力します。例えば、2 などです。
Unused VLAN for Hopping	未使用の VLAN をネイティブ VLAN として入力します。

Authentication Proxy-IOS

ネットワークにログインしたり、HTTP を使用してインターネットにアクセスし、VPN 機能用に設定されている Cisco IOS デバイスの認証プロキシ システム定義済み設定テンプレートの展開を容易にするには、このオプションを使用します。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Templates] > [CLI Templates] > [System Templates - CLI] > [Authentication Proxy-IOS] にある [Template Detail] の各フィールドについて説明します。

表 2-92　[CLI Templates] > [System Templates - CLI] > [Authentication Proxy-IOS]

フィールド	説明
AAA Action	必要なオプションを有効または無効にする場合に選択します。変更を加えない場合は、[No Change] を選択します。
AAA Method1	認証の最初の方式として [TACACS+] または [RADIUS] のいずれかを選択します。設定しない場合は、[None] を選択します。
AAA Method2	最初の方式の選択に基づき、2 番目の認証方式として [TACACS+] または [RADIUS] のいずれかを選択します。設定しない場合は、[None] を選択します。
Cache Timeout in Minutes	タイムアウト値。デフォルトのタイムアウト値の範囲は 1 ～ 2147483647 です。デフォルト値は 60 です。
Banner Action	ログイン ページのバナー表示を設定またはリセットするには、[Enable] または [Disable] を選択します。 • [Enable] を選択した場合は、ログイン ページにルータ名が表示されます。 • [Disable] を選択した場合は、ルータ名は表示されません。 バナーに変更を加えない場合は、[No Change] を選択します。
Banner Text	ログイン後にバナーに表示するテキストを入力します。バナー テキストを入力した場合、ルータ名ではなく、このテキストがログイン ページに表示されます。 これはオプションのフィールドです。
Authentication Proxy Rule Action	認証プロキシ規則を有効または無効にします。 • [Enable] を選択した場合は、名前付きの認証プロキシ規則が作成され、アクセス リストに関連付けられます。 • [Disable] を選択した場合は、関連付けられているプロキシ規則が削除されます。 フィールドの認証プロキシ規則グループに変更を加えない場合は、[No Change] を選択します。
Authentication Proxy Rule Name	認証プロキシ規則の名前を入力します。 名前には 16 文字以内の英数字を使用できます。

表 2-92　[CLI Templates] > [System Templates - CLI] > [Authentication Proxy-IOS]（続き）

フィールド	説明
Authentication Proxy Rule Overriding Timeout	デフォルトのキャッシュ タイムアウトを上書きするタイムアウト値を入力します。 これはオプションのフィールドです。上書きするタイムアウト値は 1 ～ 2147483647 の範囲にする必要があります。
Authentication Proxy Rule ACL Number/Name	認証プロキシと一緒に使用する標準アクセス リストの名前または番号を入力します。 これはオプションのフィールドです。
New Model [AAA] Action	AAA を有効または無効にするために必要なオプションを選択します。

Banner Configuration-IOS

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Templates] > [CLI Templates] > [System Templates - CLI] > [Banner Configuration-IOS] にある [Template Detail] の各フィールドについて説明します。

表 2-93　[CLI Templates] > [System Templates - CLI] > [Banner Configuration-IOS]

フィールド	説明
[Form View] タブ	
Motd Action	デイ バナーのメッセージを追加または削除する適切なオプションを選択します。既存のタスクを変更ない場合や、このフィールドの値を変更したくない場合は、[No Change] を選択します。
Motd Message	[Action] フィールドで [Add] を選択した場合は、メッセージを入力します。ユーザがルータに接続すると、ログイン プロンプトよりも前に、Message-of-The-Day（Motd）バナーが表示されます。
Exec Action	Exec バナーを追加または削除する適切なオプションを選択します。既存のタスクを変更ない場合や、このフィールドの値を変更したくない場合は、[No Change] を選択します。
Exec Message	[Action] フィールドで [Add] を選択した場合は、メッセージを入力します。ユーザがルータにログインした後に、Exec バナーまたは着信バナーが表示されます。
Incoming Action	着信バナーを追加または削除する適切なオプションを選択します。既存のタスクを変更ない場合や、このフィールドの値を変更したくない場合は、[No Change] を選択します。
Incoming Message	[Action] フィールドで [Add] を選択した場合は、メッセージを入力します。ユーザがルータに正常にログインした後に、Exec バナーまたは着信バナーが表示されます。
Login Action	ログイン バナーを追加または削除する適切なオプションを選択します。既存のタスクを変更ない場合や、このフィールドの値を変更したくない場合は、[No Change] を選択します。
Login Message	[Action] フィールドで [Add] を選択した場合は、メッセージを入力します。ユーザがルータに接続すると、最初に Motd バナーが表示され（設定されている場合）、続いてログイン バナーとプロンプトが表示されます。
Slip_PPP Action	Slip/PPP バナーを追加または削除する適切なオプションを選択します。既存のタスクを変更ない場合や、このフィールドの値を変更したくない場合は、[No Change] を選択します。
Slip_PPP Message	[Action] フィールドで [Add] を選択した場合は、カスタムの SLIP または PPP 接続メッセージを入力します。これは、レガシー クライアント アプリケーションに専用の接続文字列が必要な場合に役立ちます。

Certificate Authority-IOS

このテンプレートでは、VPN デバイスの IP セキュリティ標準の管理性および拡張性を指定できます。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Templates] > [CLI Templates] > [System Templates - CLI] > [Certificate Authority-IOS] にある [Template Detail] の各フィールドについて説明します。

表 2-94　[CLI Templates] > [System Templates - CLI] > [Certificate Authority-IOS]

フィールド	説明
[Form View] タブ	
Certificate Authority Action	認証局（CA）をアクティブ化または非アクティブ化するには、[Enable] または [Disable] を選択します。 • [Enable] を選択した場合は、CA を作成または変更できます。 • [Disable] を選択した場合は、CA を削除できます。
Certificate Authority Name	CA 名を入力します。この名前が、設定する認証強を識別するために使用されます。 この名前は、CA ドメイン名です。
Enrollment URL Action	• [Value] フィールドで指定した URL を使用してルータが CA に接続できるようにするには、[Enable] を選択します。 • CA に接続しない場合は、[Disable] を選択します。 • [Enrollment URL] フィールドを変更せずにそのままにするには、[No Change] を選択します。
Enrollment URL Value	CA の URL を入力します。 URL には、利用可能な非標準 cgi-bin スクリプトの場所が含まれている必要があります。
Enrollment Mode Action	• CA が登録局（RA）を提供する場合は、[Enable] を選択します。 • 指定した LDAP サーバを無効にするには、[Disable] を選択します。 • [Enrollment Mode] フィールドを変更せずにそのままにするには、[No Change] を選択します。
Enrollment Mode LDAP Server	CA システムが RA を提供する場合は、CA の LDAP サーバを入力します。 LDAP サーバには CRL（証明書失効リスト）の場所と証明書が含まれています。
Enrollment Retry Period in Minutes	証明書要求の次の再試行までの待機時間を入力します。 待機時間は、1 ～ 60 分です。 デフォルトの待機時間を 1 分に設定するには、このオプションを選択します。
Enrollment Retry Count Number	証明書要求の再試行回数を入力します。 再試行回数は 1 ～ 100 にする必要があります。 デフォルトの再試行時間を 1 分に設定するには、このオプションを選択します。
CRL Optional Action	証明書失効リストを確認するには、[Enable] を選択します。 [Disable] を選択した場合は、証明書失効リストは確認されません。 変更を加えない場合は、[No Change] を選択します。

表 2-94　[CLI Templates] > [System Templates - CLI] > [Certificate Authority-IOS]（続き）

フィールド	説明
Certificate Query Action	証明書クエリを有効または無効にする場合、あるいは変更を加えないは場合にこのオプションを選択します。 • [Enable] を選択した場合、証明書クエリがルータ上のすべてのトラスト ポイントに追加されます。 • [Disable] を選択した場合は、証明書に問い合わせは行われません。
RSA Key pairs Action	RSA キー ペアを生成または削除する場合、あるいは変更を加えない場合にこのオプションを選択します。この機能で、Cisco IOS ルータが複数のキー ペアを持てるように設定できます。 したがって、Cisco IOS ソフトウェアはアイデンティティ証明書ごとに異なるキー ペアを維持できます。
RSA Key pairs Key Type	次の中からキー タイプを指定します。 • [General Purpose]:暗号化と署名の両方に使用する汎用キー ペアを生成します。 • [Usage]:ドキュメントの暗号化および署名に別個の使用状況キーを生成します。
Enter number of modulus bits	署名キーについては、キー係数のサイズを 360 ～ 4096 の範囲で選択します。512 を超えるキー係数を選択すると、数分かかる場合があります。

Core Layer-IOS

プラットフォーム、LAN スイッチのユニバーサル設定、コア スイッチのグローバル設定、IP マルチキャスト ルーティングを設定し、デバイスをディストリビューション レイヤに接続するには、このオプションを使用します。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Templates] > [CLI Templates] > [System Templates - CLI] > [Core Layer-IOS] にある [Template Detail] の各フィールドについて説明します。

表 2-95　[CLI Templates] > [System Templates - CLI] > [Core Layer-IOS]

フィールド	説明
[Form View] タブ	
Configure LAN Switch Universal Setting	
Host name	LAN スイッチのユニバーサル設定のホスト名を入力します。
IP Domain-name	非完全修飾ホスト名（ドット付き 10 進表記ドメイン名のない名前）を完成させるために Cisco IOS ソフトウェアが使用する、デフォルトのドメイン名を入力します。ドメイン名を未修飾の名前から区切るために使用される最初のピリオドは入れないでください。
SNMP-server community RO	Simple Network Management Protocol（SNMP）へのアクセスを許可するコミュニティ アクセス文字列を設定する、SNMP サーバ コミュニティの読み取り専用アクセス（RO）を入力します。

表 2-95　[CLI Templates] > [System Templates - CLI] > [Core Layer-IOS]（続き）

フィールド	説明
SNMP-server community RW	Simple Network Management Protocol(SNMP)へのアクセスを許可するコミュニティ アクセス文字列を設定するには、SNMP サーバ コミュニティの読み取り/書き込みアクセス権(RW)を入力します。
Enable Secret Password	自動的に暗号化を実行するには、[Enable Secret Password] コマンドを入力します。
Username Admin Password	ユーザ名管理パスワードを入力します。
IP Address of Tacacs Server	TACACS サーバの IP アドレスを入力します。
TACACS Key	スイッチを TACACS サーバに対して認証するには、TACACS 秘密キーを入力します。
NTP Server IP Address	アプリケーションやその他のデスクトップ プロセスのクロックの同期を保持するために、NTP サーバの IP アドレスを入力します。
Time Zone	新しい夏時間(DST)の変更に適合するには、タイム ゾーンを入力します。
Hours offset from UTC	協定世界時間(UTC)から遅れている、または進んでいる時間数を選択します。
Minutes offset from UTC	協定世界時間(UTC)から遅れている、または進んでいる分数を入力します。
Summer Time zone	夏時間を入力します。
Configure the Core Switch Global Settings	
Loopback-1 IP Address	ループバック 1 の IP アドレスを入力します。
Loopback-2 IP Address	ループバック 2 の IP アドレスを入力します。
Autonomous System Number	ネットワークを一意に識別する自律システム番号を入力します。
Network Address	ネットワーク アドレスを入力します。
Inverse Mask	逆マスクを入力します。
IP address of Rendezvous-point	マルチキャスト データの送信元と受信側が接触する場所として機能するランデブー ポイント(RP)の IP アドレスを入力します。
Access List Number	アクセス リスト番号を入力します。
Multicast Network	マルチキャスト ネットワークのアドレスを入力します。
Multicast Inverse Mask	マルチキャストの逆マスクのアドレスを入力します。
Other Setting	
MSDP Core Switch IP Address to Configure IP Multicast Routing	さまざまなドメイン内のすべてのランデブー ポイント(RP)にグループのマルチキャスト送信元を通知するには、Multicast Source Discovery Protocol (MSDP)を入力します。
Connecting to Distribution Layer	
Port Channel Number	ポート チャネル番号を入力します。
Port Channel IP Address	ポート チャネルの IP アドレスを入力します。
Port Channel Subnet Mask <ポート チャネルのネットワーク マスクとして表示>	ポート チャネルのサブネット マスクを入力します。

表 2-95　[CLI Templates] > [System Templates - CLI] > [Core Layer-IOS]（続き）

フィールド	説明
TenGigabitEthernet First Interface Number	TenGigabitEthernet の最初のインターフェイス番号を入力します。
TenGigabitEthernet Second Interface Number	TenGigabitEthernet の 2 番目のインターフェイス番号を入力します。

Crypto Map Configuration-IOS

デバイスで IPsec を設定するには、このオプションを選択します。IKE とトランスフォームを設定してから、このテンプレートを設定する必要があります。そうすることで、VPN 対応デバイスにのみダウンロードできます。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Templates] > [CLI Templates] > [System Templates - CLI] > [Crypto Map Configuration-IOS] にある [Template Detail] の各フィールドについて説明します。

表 2-96　[CLI Templates] > [System Templates] - [CLI] > [Crypto Map Configuration-IOS]

フィールド	説明
[Form View] タブ	
Crypto Map Action	Cisco IOS 設定を追加または削除するオプションを選択します。
Crypto Map Name	暗号マップの名前を入力します。
Map Number	暗号マップの番号を入力します。 1 ～ 65535 の範囲で値を入力する必要があります。
Map Type	暗号マップのマップ タイプ（手動か ISAKMP か）を選択します。 • [Manual]：通常、手動キーイングは、インターネット キー エクスチェンジ（IKE）をサポートしない別のベンダーのデバイスに対してトラフィックを暗号化するようにシスコ デバイスを設定する場合にのみ必要です。 • [ISAKMP]：ISAKMP は、インターネット キー管理用のフレームワークを提供し、セキュリティ属性のネゴシエーションに特定のプロトコル サポートを提供します。
Map Description	暗号マップの説明を入力します。
Crypto ACL	暗号マップの拡張アクセス リストを入力します。
IPSec Peer	暗号マップに関連付ける IPsec のピア ホスト名または IP アドレスを入力します。
Transform Set Name	暗号マップで使用するトランスフォーム セット名を入力します（[Security] > [VPN Components] > [Transform Sets]（2-92 ページ）を参照）。

DNS Configuration-IOS

Cisco IOS デバイスでドメイン ネーム システム（DNS）を設定するには、このオプションを使用します。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Templates] > [CLI Templates] > [System Templates - CLI] > [DNS Configuration-IOS] にある [Template Detail] の各フィールドについて説明します。

表 2-97　[CLI Templates] > [System Templates - CLI] > [DNS Configuration-IOS]

フィールド	説明
[Form View] タブ	
Add DNS Servers	追加する DNS ネーム サーバの IPv4 アドレス/IPv6 アドレスを入力します。 複数のアドレスを指定する場合は、カンマで区切ります。 デバイスが許可する DNS サーバが 1 つだけの場合は、最初のアドレスが考慮されます。
Remove DNS Servers	削除する DNS ネーム サーバの IPv4 アドレス/IPv6 アドレスを入力します。 複数のアドレスを指定する場合は、カンマで区切ります。
Remove Domain Name	ドメイン名を削除するには、このオプションを選択します。 変更を加えない場合は、[No Change] を選択します。
Domain Name	削除する DNS ネーム サーバの IP アドレスを入力します。 複数のアドレスを指定する場合は、カンマで区切ります。
Domain Lookup	IP DNS ベースのホスト名からアドレスへの変換を有効または無効にする場合に選択します。 変更を加えない場合は、[No Change] を選択します。
CLNS NSAP	CLNS NSAP オプションを有効または無効にする場合、あるいは変更を加えない場合に選択します。このオプションを有効にすると、指定した CLNS NSAP プレフィックスを持つパケットは CLNS（Connectionless Network Service）プロトコルをルータが検出されなかったかのように動作させます。 変更を加えない場合は、[No Change] を選択します。
OSPF	OSPF（Open Shortest Path First）プロトコル オプションを有効または無効にする場合、あるいは変更を加えない場合に選択します。 変更を加えない場合は、[No Change] を選択します。
Domain List Action	ドメイン リストを追加または削除する場合、あるいは変更を加えない場合に選択します。 変更を加えない場合は、[No Change] を選択します。
Domain List	不完全なホスト名を完全にするか、既存のリストに追加するにはドメイン名を入力します。 複数のドメイン名はカンマで区切ります。 最初のピリオドはドメイン名の前に入れないでください。

DNS Configuration-NAM

NAM カテゴリ デバイスでドメイン ネーム システム（DNS）を設定するには、このオプションを使用します。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Templates] > [CLI Templates] > [System Templates - CLI] > [DNS Configuration-NAM] にある [Template Detail] の各フィールドについて説明します。

表 2-98　[CLI Templates] > [System Templates - CLI] > [DNS Configuration-NAM]

フィールド	説明
[Form View] タブ	
Add DNS Servers	追加する DNS ネーム サーバの IPv4 アドレスを入力します。 複数のアドレスを指定する場合は、カンマで区切ります。 デバイスが許可する DNS サーバが 1 つだけの場合は、最初のアドレスが考慮されます。
Remove Domain Name	ドメイン名を削除するには、このオプションを選択します。
Domain Name	削除する DNS ネーム サーバの IP アドレスを入力します。 複数のアドレスを指定する場合は、カンマで区切ります。
Disable Name Servers	ドメイン ネーム サーバを無効にする場合に選択します。

DNS Configuration-Nexus

Nexus カテゴリ デバイスでドメイン ネーム システム（DNS）を設定するには、このオプションを使用します。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Templates] > [CLI Templates] > [System Templates - CLI] > [DNS Configuration-Nexus] にある [Template Detail] の各フィールドについて説明します。

表 2-99　[CLI Templates] > [System Templates - CLI] > [DNS Configuration-Nexus]

フィールド	説明
[Form View] タブ	
Add DNS Servers	追加する DNS ネーム サーバの IPv4 アドレス/IPv6 アドレスを入力します。 複数のアドレスを指定する場合は、カンマで区切ります。 デバイスが許可する DNS サーバが 1 つだけの場合は、最初のアドレスが考慮されます。
Remove DNS Servers	削除する DNS ネーム サーバの IPv4 アドレス/IPv6 アドレスを入力します。 複数のアドレスを指定する場合は、カンマで区切ります。
Remove Domain Name	ドメイン名を削除するには、このオプションを選択します。
Domain Name	削除する DNS ネーム サーバの IP アドレスを入力します。 複数のアドレスを指定する場合は、カンマで区切ります。
Domain Lookup	IP DNS ベースのホスト名からアドレスへの変換を有効または無効にする場合に選択します。 変更を加えない場合は、[No Change] を選択します。

表 2-99　[CLI Templates] > [System Templates - CLI] > [DNS Configuration-Nexus]（続き）

フィールド	説明
Domain List Action	ドメイン リストを追加または削除する場合、あるいは変更を加えない場合に選択します。 変更を加えない場合は、[No Change] を選択します。
Domain List	不完全なホスト名を完全にするか、既存のリストに追加するにはドメイン名を入力します。 複数のドメイン名はカンマで区切ります。 最初のピリオドはドメイン名の前に入れないでください。

Distribution Layer-IOS

プラットフォームの設定、LAN スイッチのユニバーサル設定、ディストリビューションのグローバル設定を行い、デバイスをアクセス レイヤおよび LAN コアまたは WAN ルータに接続するには、このオプションを使用します。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Templates] > [CLI Templates] > [System Templates - CLI] > [Distribution Layer-IOS] にある [Template Detail] の各フィールドについて説明します。

表 2-100　[CLI Templates] > [System Templates - CLI] > [Distribution Layer-IOS]

フィールド	説明
[Form View] タブ	
Device Type	選択したデバイス タイプにのみテンプレートを展開します。 **注**　展開上の問題を避けるため、このフィールドは編集しないでください。
Device OID	選択したデバイス OID にのみテンプレートを展開します。 **注**　展開上の問題を避けるため、このフィールドは編集しないでください。
Switch Number	スイッチ番号を入力します。
LAN Switch Universal Configuration	
Host name	LAN スイッチのユニバーサル設定のホスト名を入力します。
IP Domain-name	非完全修飾ホスト名（ドット付き 10 進表記ドメイン名のない名前）を完成させるために Cisco IOS ソフトウェアが使用する、デフォルトのドメイン名を入力します。ドメイン名を未修飾の名前から区切るために使用される最初のピリオドは入れないでください。
SNMP-server community RO	Simple Network Management Protocol（SNMP）へのアクセスを許可するコミュニティ アクセス文字列を設定する、SNMP サーバ コミュニティの読み取り専用アクセス（RO）を入力します。
SNMP-server community RW	Simple Network Management Protocol（SNMP）へのアクセスを許可するコミュニティ アクセス文字列を設定するには、SNMP サーバ コミュニティの読み取り/書き込みアクセス権（RW）を入力します。
Enable Secret Password	自動的に暗号化を実行するには、[Enable Secret Password] コマンドを入力します。
Username Admin Password	ユーザ名管理パスワードを入力します。
IP Address of Tacacs Server	TACACS サーバの IP アドレスを入力します。

表 2-100　[CLI Templates] > [System Templates - CLI] > [Distribution Layer-IOS]（続き）

フィールド	説明
TACACS Key	スイッチを TACACS サーバに対して認証するには、TACACS 秘密キーを入力します。
NTP Server IP Address	アプリケーションやその他のデスクトップ プロセスのクロックの同期を保持するために、NTP サーバの IP アドレスを入力します。
Time Zone	新しい夏時間（DST）の変更に適合するには、タイム ゾーンを入力します。
Hours offset from UTC	協定世界時間（UTC）から遅れている、または進んでいる時間数を選択します。
Minutes offset from UTC	協定世界時間（UTC）から遅れている、または進んでいる分数を入力します。
Summer Time zone	夏時間を入力します。
Distribution Global Settings Configuration	
Loopback-1 IP Address	ループバック 1 の IP アドレスを入力します。
IP address of Rendezvous-point	マルチキャスト データの送信元と受信側が接触する場所として機能するランデブー ポイント（RP）の IP アドレスを入力します。
Multicast Network Address	マルチキャスト ネットワークのアドレスを入力します。
Network Address	ネットワーク アドレスを入力します。
Inverse Mask	逆マスクのアドレスを入力します。
Autonomous System Number	各ネットワークを一意に識別する自律システム番号を入力します。
Other Setting	
Access List Number	アクセス リスト番号を入力します。
Connecting to Access Layer	
Data VLAN	ユーザ生成トラフィックのみを搬送するには、データ VLAN を入力します。
Voice VLAN	IP 電話からの IP 音声トラフィックを搬送するアクセス ポートを有効にするには、音声 VLAN を入力します。
Management VLAN	ネットワークで使用される IP アドレス空間を検出、モニタ、監査、および管理するための管理 VLAN を入力します。
Unused VLAN for Hopping	ホッピングを防ぐため、未使用の VLAN をネイティブ VLAN として入力します。
Channel Group Number	EtherChannel インターフェイスを EtherChannel グループに割り当てて設定するには、チャネル グループ番号を入力します。
Interface Type	ドロップダウンリストからインターフェイス タイプを選択します。
TenGigabitEthernet First Interface Number	TenGigabitEthernet の最初のインターフェイス番号を入力します。
TenGigabitEthernet Second Interface Number	TenGigabitEthernet の 2 番目のインターフェイス番号を入力します。
DHCP Server IP Address	ネットワーク デバイスに IP アドレスを割り当てるには、Dynamic Host Configuration Protocol（DHCP）の IP アドレスを入力します。
Data VLAN IP Address	データ VLAN の IP アドレスを入力します。
Data VLAN IP Mask	データ VLAN の IP マスクを入力します。
Voice VLAN IP Address	音声 VLAN の IP アドレスを入力します。
Voice VLAN IP Mask	音声 VLAN の IP マスクを入力します。

表 2-100　[CLI Templates] > [System Templates - CLI] > [Distribution Layer-IOS]（続き）

フィールド	説明
Management VLAN IP Address	管理 VLAN の IP アドレスを入力します。
Management VLAN IP Mask	管理 VLAN の IP マスクを入力します。
Connecting to LAN Core or WAN Router	
Port Channel Number	ポート チャネル番号を入力します。
Port Channel IP Address	ポート チャネルの IP アドレスを入力します。
Port Channel Subnet Mask	ポート チャネルのサブネット マスクを入力します。
Network Address	ネットワーク アドレスを入力します。
Network Subnet Mask	ネットワークのサブネット マスクを入力します。
Interface Type	ドロップダウンリストからインターフェイス タイプを選択します。
Start Interface Number	LAN コアまたは WAN ルータに接続するための開始インターフェイス番号を入力します。
End Interface Number	LAN コアまたは WAN ルータに接続するための終了インターフェイス番号を入力します。

EEM Environmental Variables-IOS

Cisco IOS デバイスで Embedded Event Manager（EEM）TCL スクリプト ポリシーによって使用される EEM の環境変数を設定するには、このオプションを使用します。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Templates] > [CLI Templates] > [System Templates - CLI] > [EEM Environmental Variables-IOS] にある [Template Detail] の各フィールドについて説明します。

表 2-101　[CLI Templates] > [System Templates - CLI] > [EEM Environmental Variables-IOS]

フィールド	説明
[Form View] タブ	
Action	次のいずれかを選択します。 • [Add]：1 つ以上の変数を追加します。 または • [Remove]：1 つ以上の変数を削除します。
Variable Name	変数の名前を入力します。 例： `my_counter` 一度に最大 5 つの変数を作成できます。
Variable Value	変数の値を入力します。 例： `15` これで、変数 `my_counter` の値は `15` になります。

注　5 つの変数名と変数値を一度に入力できます。6 つ以上の変数名と値を入力するには、テンプレートを再度展開する必要があります。

Embedded Event Manager Configuration-IOS

Cisco IOS デバイスで Embedded Event Manager（EEM）スクリプトまたはアプレットを設定するには、このオプションを使用します。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Templates] > [CLI Templates] > [System Templates - CLI] > [Embedded Event Manager Configuration-IOS] にある [Template Detail] の各フィールドについて説明します。

表 2-102　[CLI Templates] > [System Templates - CLI] > [Embedded Event Manager Configuration-IOS]

フィールド	説明
[Form View] タブ	
EEM Configuration Action	スクリプトまたはアプレットを登録または登録解除するには、[Register] または [Unregister] を選択します。
EEM Configuration Policy Type	ポリシーとして [Script] または [Applet] のいずれかを選択します。 ポリシー タイプとしてスクリプトを選択した場合は、次のフィールドに入力します。 • Create New Directory • Directory Name • Enter the Server Name • Enter the Script File Location with Name ポリシー タイプとしてアプレットを選択した場合は、次のフィールドに入力します。 • Enter the Applet Name • Enter the Applet File Content
Create New Directory	スクリプトをコピーするデバイスに新しいディレクトリを作成する場合は、このオプションをオンにします。 このチェックボックスをオンにすると、[Directory Name] テキスト ボックスに指定した入力を使用して新しいディレクトリが作成されます。
Directory Name	ファイルを配置する必要があるデバイス上のディレクトリの絶対パスを入力します。 例: `disk0:/Testing` ここでは、disk0 パーティションの下のデバイスに新しいディレクトリの Testing が作成されます。 スクリプト ファイルをコピーする前に、選択したディレクトリに十分な容量があることを確認してください。

表 2-102　[CLI Templates] > [System Templates - CLI] > [Embedded Event Manager Configuration-IOS]（続き）

フィールド	説明
Enter the Server Name	TFTP サーバ名を入力します。 **注**　スクリプト ファイルは TFTP 起動フォルダ内で利用可能である必要があります。
Enter the Script File Location	デバイスに展開するためにスクリプトをアップロードするファイルの場所を入力するには、このオプションを使用します。 絶対パスとファイル名を入力する必要があります。 **注**　指定できるスクリプト ファイルは 1 つだけです。
Enter the Applet Name	EEM の設定アクションとして [Unregister] を選択した場合は、アプレット名を入力します。
Enter the Applet File Content	EEM の設定アクションとして [Register] を選択した場合は、アプレット ファイルのコンテンツを入力します。

Enable Password-IOS

有効化パスワード、またはシークレット パスワードを設定し、Cisco IOS デバイスでイネーブル モードに入るには、このオプションを使用します。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Templates] > [CLI Templates] > [System Templates - CLI] > [Enable Password-IOS] にある [Template Detail] の各フィールドについて説明します。

表 2-103　[CLI Templates] > [System Templates - CLI] > [Enable Password-IOS]

フィールド	説明
[Form View] タブ	
Action	有効化パスワードを有効または無効にする場合、あるいは変更を加えないは場合にこのオプションを選択します。 変更を加えない場合は、[No Change] を選択します。
Enable Password	有効化パスワードを入力します。
Password Level	有効化パスワードのレベルを設定します。レベルは 1 ～ 100 の範囲で指定できます。 Cisco IOS デバイスの場合、パスワードを有効にしても、Cisco IOS デバイスがイネーブル モードになれないため、有効化パスワードも、イネーブル シークレット パスワードも無効にしないことをお勧めします。デバイスのコンソール パスワードがある場合にのみ、これを行うことができます。 [Common Parameters] ペインで有効化パスワードに [No Change] を選択し、[IOS Parameters] ペインでイネーブル シークレットに [Disable] を選択した場合は、デバイスおよびクレデンシャル データベースのイネーブル シークレット パスワードが更新されます。 [Common Parameters] ペインで有効化パスワードに [Disable] を選択し、[IOS Parameters] ペインでイネーブル シークレットに [No Change] を選択した場合は、デバイスおよびクレデンシャル データベースの有効化パスワードが更新されます。
Encrypted	パスワードを暗号化するには、このオプションを選択します。
Secret Action	シークレット パスワードを有効または無効にする場合、あるいは変更を加えないは場合にこのオプションを選択します。

表 2-103　[CLI Templates] > [System Templates - CLI] > [Enable Password-IOS]（続き）

フィールド	説明
Secret Password	シークレット パスワードを入力します。
Level	パスワード レベルを設定します。1 ～ 15 の レベルを指定できます。
Encrypted	パスワードを暗号化するには、このオプションを選択します。

GOLD Boot Level and Monitoring Test for Cat6k Devices-IOS

ゴールドの起動レベルとモニタリングテストを Cat6k デバイス上で設定するには、このオプションを使用します。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Templates] > [CLI Templates] > [System Templates - CLI] > [GOLD Boot Level And Monitoring Test for Cat6k Devices-IOS] にある [Template Detail] の各フィールドについて説明します。

表 2-104　[CLI Templates] > [System Templates-CLI] > [GOLD Boot Level and Monitoring Test for Cat6k Devices-IOS]

フィールド	説明
Gold Boot Level Configuration Action	アクションを有効にするには [Enable]、アクションを無効にするには [Disable] を選択します。
Gold Bootup Level	起動レベルを完全に設定するには [Complete]、起動レベルを最小に設定するには [Minimal] を選択します。
GOLD Monitoring Test Action	次のいずれかをオンにします。 • [Addinterval]：間隔を追加します。 • [Nointerval]：間隔を追加しません。 ゴールドのモニタリング テストのアクションに変更を加えない場合は、[No Change] を選択します。
GOLD Monitoring Test Module Number	選択したデバイス内のゴールドのモニタリング テストのモジュール番号を入力します。カンマで区切ると、複数のモジュール番号を入力できます。
Tests Details Action	次のいずれかをオンにします。 • [All]：すべての診断テストを設定できるようにします。 • [Testnames]：テスト名を手動で入力できるようにします。 • [TestRange]：実行するテストの範囲を入力できるようにします。
Test Names	カンマで区切ると、複数のテスト名を入力できます。カンマの間にスペースを入れないでください。アクションが [Testnames] の場合、このフィールドは必須です。
Range	テスト範囲を入力します。アクションが [TestRange] の場合、このフィールドは必須です。
No. of Days To Configure Health Monitoring Interval	デバイスでテストを実行するまでの日数を入力します。日数には 0 ～ 20 の任意の値を入力できます。
Begin Time To Configure Health Monitoring Interval	テストを実行する頻度を時間、分、秒単位で入力します。

表 2-104　[CLI Templates] > [System Templates-CLI] > [GOLD Boot Level and Monitoring Test for Cat6k Devices-IOS]（続き）

フィールド	説明
Configuring Health Monitoring Interval in Milliseconds	テストを実行するミリ秒単位の頻度を入力します。秒は 0 ～ 999 の任意の値を入力できます。
Enable/Disable Health Monitoring Diagnostics Test Action	次のいずれかをオンにします。 • [Enable]：ヘルス モニタリング テストを開始します。 • [Disable]：実行しているヘルスモニタリング テストを停止します。 ヘルス モニタリング テストのアクションに変更を加えない場合は、[No Change] を選択します。

GOLD Monitoring Test for Non Stack Devices-IOS

ゴールドのモニタリング テストを非スタック デバイス上で設定するには、このオプションを使用します。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Templates] > [CLI Templates] > [System Templates - CLI] > [GOLD Monitoring Test for Non Stack Devices-IOS] にある [Template Detail] の各フィールドについて説明します。

表 2-105　[CLI Templates] > [System Templates - CLI] > [GOLD Monitoring Test for Non Stack Devices-IOS]

フィールド	説明
Non Stack Health Monitor Action	次のいずれかをオンにします。 • [Addinterval]：間隔を追加します。 • [Nointerval]：間隔を追加しません。 非スタック ヘルス モニタのアクションに変更を加えない場合は、[No Change] を選択します。
Non Stack Tests Details Action	次のいずれかをオンにします。 • [All]：すべての診断テストを設定できるようにします。 • [Testnames]：テスト名を手動で入力できるようにします。 • [TestRange]：実行するテストの範囲を入力できるようにします。

注　同様のフィールドの説明については、表 2-104（2-128 ページ）を参照してください。

GOLD Monitoring Test for Stack Enabled Devices-IOS

ゴールドのモニタリング テストをスタック対応デバイス上で設定するには、このオプションを使用します。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Templates] > [CLI Templates] > [System Templates - CLI] > [GOLD Monitoring Test for Stack Enabled Devices-IOS] にある [Template Detail] の各フィールドについて説明します。

表 2-106　[CLI Templates] > [System Templates - CLI] > [GOLD Monitoring Test for Stack Enabled Devices-IOS]

フィールド	説明
Stack Health Monitor Action	次のいずれかをオンにします。 • [Addinterval]:間隔を追加します。 • [Nointerval]:間隔を追加しません。 スタック ヘルス モニタのアクションに変更を加えない場合は、[No Change] を選択します。
Stack Health Monitor Switch Id(s)	スイッチ ID を入力します。単一のスイッチ ID を入力したり、複数のスイッチ ID をカンマで区切って入力したりできます。例 1:ID 2 のスイッチを含める場合は 2 と入力します。例 2:ID 3 と 6 のスイッチを含める場合は 3, 6 と入力します。
Stack Tests Details Action	次のいずれかをオンにします。 • [All]:すべての診断テストを設定できるようにします。 • [Testnames]:テスト名を手動で入力できるようにします。 • [TestRange]:実行するテストの範囲を入力できるようにします。

注　同様のフィールド説明については、表 2-104(2-128 ページ)を参照してください。

HTTP-HTTPS Server and WSMA Configuration-IOS

デバイスで HTTP アクセスを設定し、次に WSMA および VPN の機能を設定するには、このオプションを使用します。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Templates] > [CLI Templates] > [System Templates - CLI] > [HTTP-HTTPS Server and WSMA Configuration-IOS] にある [Template Detail] の各フィールドについて説明します。

表 2-107　[CLI Templates] > [System Templates - CLI] > [HTTP-HTTPS Server and WSMA Configuration-IOS]

フィールド	説明
Server Action	デバイスでの HTTP または HTTPs のアクセスを有効または無効にするオプションを選択します。サーバのアクションに変更を加えない場合は、[No Change] を選択します。
Port Number	HTTP または HTTPS サーバのポート番号を 1024 ～ 65535 までの範囲で指定します。デフォルトの HTTP ポート番号は 80、デフォルトの HTTPS ポート番号は 443 です。

表 2-107　[CLI Templates] > [System Templates - CLI] > [HTTP-HTTPS Server and WSMA Configuration-IOS]（続き）

フィールド	説明
Authentication Action	認証方式を有効または無効にするオプションを選択します。認証のアクションに変更を加えない場合は、[No Change] を選択します。
Authentication Method	認証方式を選択します。 • aaa • Enable • local • tacacs
Access List Action	アクセス リストを有効または無効にするオプションを選択します。アクセス リストのアクションに変更を加えない場合は、[No Change] を選択します。
ACL Number/Name	使用するアクセス コントロール リストの番号または名前を入力します。アクセス リストの番号は 1 ～ 99 にする必要があります。
WSMA Action	WSMA アクションを有効または無効にするオプションを選択します。WSMA のアクションに変更を加えない場合は、[No Change] を選択します。

Cisco IOS デバイスに [HTTP-HTTPS Server and WSMA Configuration-IOS] テンプレートを適用するには、次の手順を実行します。

テンプレートに 2 つのインスタンスを作成します。つまり、指定したテンプレートを編集し、そのテンプレートを HTTP-WSMA-For-ISR-ASR-Series として（WSMA を有効/無効として）保存し、再度、そのテンプレートを別の名前で編集して保存できます。

注　ISR、ISR-G2、および ASR シリーズのルータを有効にする必要があります。その他のルータの [WSMA] オプションは [No Change] のままにしてください。

MAC Trap Configuration

SNMPv1 または SNMPv2 のMAC 通知トラップをスイッチで有効にするには、このオプションを使用します。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Templates] > [CLI Templates] > [System Templates - CLI] > [MAC Trap Configuration] にある [Template Detail] の各フィールドについて説明します。

表 2-108　[CLI Templates] > [System Templates - CLI] > [MAC Trap Configuration]

フィールド	説明
Device OID	選択したデバイス OID にのみテンプレートを展開します。 **注**　展開上の問題を避けるため、このフィールドは編集しないでください。
Notification Interval	トラップの間隔を 0 ～ 2147483647 の秒単位で入力します。
Host Name/IP Address	トラップ受信側のホスト名または IP アドレスを入力します。
SNMP Community	SNMP v1/v2c コミュニティ文字列を入力します。

表 2-108　[CLI Templates] > [System Templates - CLI] > [MAC Trap Configuration]（続き）

フィールド	説明
UDP Port	トラップを受信する UDP ポート番号を 0 ～ 65535 の範囲で入力します。
Interface Range	トラップを設定する必要があるインターフェイス、またはインターフェイスの範囲を入力します。

Mediatrace-Responder-Configuration

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Templates] > [CLI Templates] > [System Templates - CLI] > [-Responder-Configuration] にある [Template Detail] の各フィールドについて説明します。

表 2-109　[CLI Templates] > [System Templates - CLI] > [Mediatrace-Responder-Configuration]

フィールド	説明
Name Description	テンプレートの名前と説明（任意）を入力します。
Tags	タグを 1 つ以上入力します。 テンプレートのグループ化にはタグを使用します。テンプレートにタグを使用する方法は、次の 2 通りあります。 • テンプレートの作成時にタグを作成する。 • または、[Template] 検索バーの下にある [Tag] アイコンを使用する。
Device Type	[Routers] を選択します。
OS Version	選択したデバイス タイプの OS バージョンを入力します。これは、次の表に示す最小 Cisco IOS バージョン以降にする必要があります。このフィールドを空白のままにすると、選択したデバイス タイプ カテゴリに利用可能なすべてのタイプ（ファミリ/シリーズ/タイプ）が表示されます。

Medianet-PerfMon

Medianet のパフォーマンス モニタリングを設定するには、このオプションを使用します。[Form View] タブのフィールドはCLI テンプレートの変数として機能するため、編集できません。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Templates] > [CLI Templates] > [System Templates - CLI] > [Medianet-PerfMon] にある [Template Detail] フィールドについて説明します。

表 2-110　[CLI Templates] > [System Templates - CLI] > [Medianet-PerfMon]

フィールド	説明
Name Description	テンプレートの名前と説明(任意)を指定します。
Tags	タグを 1 つ以上入力します。 テンプレートのグループ化にはタグを使用します。テンプレートにタグを使用する方法は、次の 2 通りあります。 • テンプレートの作成時にタグを作成する。 • または、[Template] 検索バーの下にある [Tag] アイコンを使用する。
Device Type	Medianet PerfMon と互換性のあるデバイスのタイプをドロップダウン リストから 1 つ選択します。
OS Version	選択したデバイス タイプの OS バージョンを入力します。これは、次の表に示す最小 Cisco IOS バージョン以降にする必要があります。このフィールドを空白のままにすると、選択したデバイス タイプ カテゴリに利用可能なすべてのタイプ(ファミリ/シリーズ/タイプ)が表示されます。
Flow Exporter Name	選択したデバイス タイプの NetFlow エクスポータの名前。これは、文字の集合です(例:`EXPORTER-1`)。
Flow Exporter Address	Prime Infrastructure サーバの IP アドレス。
Flow Exporter Port	NetFlow モニタがエクスポートされたデータを受信するポート。上書きする特別な必要性がない限り、デフォルトの 9991 ポートを使用します。
Performance Monitor Name	フロー エクスポータからデータをキャッシングする Medianet Performance Monitor の名前(例:`MP-MONITOR-1`)。
Interface	NetFlow データをモニタするデバイス上のインターフェイスの名前(例:`ethernet 0/0`)。
Flow Monitor Name	フロー エクスポータからデータをキャッシングする NetFlow モニタの名前(例:`FLOW-MONITOR-1`)。

RADIUS Configuration-IOS

IOS デバイスに単一の RADIUS ホストまたは RADIUS グループを設定するには、このオプションを使用します。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Templates] > [CLI Templates] > [System Templates - CLI] > [Radius Configuration-IOS] にある [Template Detail] の各フィールドについて説明します。

表 2-111　[CLI Templates] > [System Templates - CLI] > [Radius Configuration-IOS]

フィールド	説明
Radius Group Name	RADIUS グループ名を入力します。
Shared Key	RADIUS サーバの認証および暗号キーを指定します。
Verify Shared Key	検証用のキーを指定します。

表 2-111 [CLI Templates] > [System Templates - CLI] > [Radius Configuration-IOS] (続き)

フィールド	説明
Server name or IP Address for Radius Group/Host	RADIUS サーバ グループ/ホストの DNS 名または IP アドレス。 単一の RADIUS ホストを入力する場合は、次のフィールドのみに入力する必要があります。 • Shared Key • Verify Shared Key • Server name or IP address for Radius Group/Host • Authentication Port • Accounting Port • Enable for 802.1X / MAB AAA • Enable AAA for Web Authentication
Authentication Port	認証要求用のポート番号を指定します。認証用とアカウンティング用のポート番号は同一にできません。ポート番号が 0 に設定されている場合、そのホストは認証に使用されません。デフォルトの認証ポート番号は 1645 です。
Accounting Port	アカウンティング要求用のポート番号を指定します。認証用とアカウンティング用のポート番号は同一にできません。ポート番号が 0 に設定されている場合、そのホストはアカウンティングに使用されません。デフォルトのアカウンティング ポート番号は 1646 です。
Server name or IP Address for Radius Group Only	RADIUS サーバ グループの DNS 名または IP アドレス。
Authentication Port	認証要求用のポート番号を指定します。認証用とアカウンティング用のポート番号は同一にできません。ポート番号が 0 に設定されている場合、そのホストは認証に使用されません。デフォルトの認証ポート番号は 1645 です。
Accounting Port	アカウンティング要求用のポート番号を指定します。認証用とアカウンティング用のポート番号は同一にできません。ポート番号が 0 に設定されている場合、そのホストはアカウンティングに使用されません。デフォルトのアカウンティング ポート番号は 1646 です。
Server name or IP Address for Radius Group Only	RADIUS サーバ グループの DNS 名または IP アドレス。
Authentication Port	認証要求用のポート番号を指定します。認証用とアカウンティング用のポート番号は同一にできません。ポート番号が 0 に設定されている場合、そのホストは認証に使用されません。デフォルトの認証ポート番号は 1645 です。
Accounting Port	アカウンティング要求用のポート番号を指定します。認証用とアカウンティング用のポート番号は同一にできません。ポート番号が 0 に設定されている場合、そのホストはアカウンティングに使用されません。デフォルトのアカウンティング ポート番号は 1646 です。
Server name or IP Address for Radius Group Only	RADIUS サーバ グループの DNS 名または IP アドレス。
Authentication Port	認証要求用のポート番号を指定します。認証用とアカウンティング用のポート番号は同一にできません。ポート番号が 0 に設定されている場合、そのホストは認証に使用されません。デフォルトの認証ポート番号は 1645 です。

表 2-111　[CLI Templates] > [System Templates - CLI] > [Radius Configuration-IOS]（続き）

フィールド	説明
Accounting Port	アカウンティング要求用のポート番号を指定します。認証用とアカウンティング用のポート番号は同一にできません。ポート番号が 0 に設定されている場合、そのホストはアカウンティングに使用されません。デフォルトのアカウンティング ポート番号は 1646 です。
Server name or IP Address for Radius Group Only	RADIUS サーバ グループの DNS 名または IP アドレス。
Authentication Port	認証要求用のポート番号を指定します。認証用とアカウンティング用のポート番号は同一にできません。ポート番号が 0 に設定されている場合、そのホストは認証に使用されません。デフォルトの認証ポート番号は 1645 です。
Accounting Port	アカウンティング要求用のポート番号を指定します。認証用とアカウンティング用のポート番号は同一にできません。ポート番号が 0 に設定されている場合、そのホストはアカウンティングに使用されません。デフォルトのアカウンティング ポート番号は 1646 です。
Enable for 802.1X / MAB AAA	802.1X および MAB 認証用の AAA を有効または無効にするために必要なオプションを選択します。
Enable AAA for Web Authentication	Web ベースの認証（WebAuth）用の AAA を有効または無効にするために必要なオプションを選択します。

Reload Configuration-IOS

Cisco IOS デバイスをリロードするには、このオプションを使用します。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Templates] > [CLI Templates] > [System Templates - CLI] > [Reload Configuration-IOS] にある [Template Detail] の各フィールドについて説明します。

表 2-112　[CLI Templates] > [System Templates - CLI] > [Reload Configuration-IOS]

フィールド	説明
Do not Save config before reload	リロードの前に設定を保存しない場合に、このオプションをオンにします。
Enter time to wait after reload	リロード後の待機時間を分単位で入力します。

Reload Configuration-NAM

NAM デバイスをリロードするには、このオプションを使用します。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Templates] > [CLI Templates] > [System Templates - CLI] > [Reload Configuration-NAM] にある [Template Detail] の各フィールドについて説明します。

表 2-113　[CLI Templates] > [System Templates - CLI] > [Reload Configuration-NAM]

フィールド	説明
Enter time to wait after reload	リロード後の待機時間を分単位で入力します。

Web User Configuration-NAM

NAM デバイスのローカル Web ユーザを作成、編集、削除するには、このオプションを使用します。

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Templates] > [CLI Templates] > [System Templates - CLI] > [Web User Configuration-NAM] にある [Template Detail] の各フィールドについて説明します。

表 2-114　[CLI Templates] > [System Templates - CLI] > [Web User Configuration-NAM]

フィールド	説明
Action	フィールドの Web ユーザ グループを追加または削除するオプションを選択します。アクションに変更を加えない場合は、[No Change] を選択します。
Username	Web ユーザのユーザ名を入力します。
Enter DES encrypted WebUser Password	ユーザ名の DES パスワードを入力します。
Account Management	アカウント管理を有効または無効にするために必要なオプションを選択します。アカウント管理に変更を加えない場合は、[No Change] を選択します。
System Config	システム設定を有効または無効にするために必要なオプションを選択します。システム設定に変更を加えない場合は、[No Change] を選択します。
Capture	キャプチャ設定を有効または無効にするために必要なオプションを選択します。キャプチャ設定に変更を加えない場合は、[No Change] を選択します。
Alarm Config	アラーム設定を有効または無効にするために必要なオプションを選択します。アラーム設定に変更を加えない場合は、[No Change] を選択します。
Collection Config	収集設定を有効または無効にするために必要なオプションを選択します。収集設定に変更を加えない場合は、[No Change] を選択します。

User Defined Protocol Configuration-NAM

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Templates] > [CLI Templates] > [System Templates - CLI] > [User Defined Protocol Configuration-NAM] にある [Template Detail] の各フィールドについて説明します。

表 2-115　[User Defined Protocol Configuration-NAM Template] ページのフィールドの説明

フィールド	説明
Action	ユーザ定義プロトコルを追加、削除、または置換するオプションを選択します。
Protocol	次のプロトコルを選択します。 • TCP • UDP
Port	ポート番号を入力します。0 ～ 65535 の範囲でポート番号を入力できます。
Name	ユーザ定義プロトコルの名前を入力します。

表 2-115　[User Defined Protocol Configuration-NAM Template] ページのフィールドの説明（続き）

フィールド	説明
Host	[Select this option to enable host]:パケットのストリームを調べます。これらのパケット（収集データ）にあるすべてのネットワーク アドレスのテーブルを生成します。 各エントリでは、ホストによって送受信されたパケットおよびバイトの合計数と、ホストによって送信された非ユニキャスト パケットの数が記録されます。
Conversations	ホスト カンバセーションを有効にするには、このオプションを選択します。
ART	アプリケーション応答時間を有効にするには、このオプションを選択します。

[Network Analysis Module]フィールドの説明

次に、[Configuration] > [Templates] ページの各フィールドについて説明します。

[Features and Technologies] >[Network Analysis Module]:

- [Network Analysis Module] > [Monitoring]
- [Network Analysis Module] > [System]

[Network Analysis Module] > [Monitoring]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Network Analysis Module] > [Monitoring] の各フィールドについて説明します。

表 2-116　[Network Analysis Module] > [Monitoring]

フィールド	説明
Response Time	[Response Time Monitor] チェックボックスをオンにし、応答時間 ResponseTime1<=ResponseTime2<=ResponseTime3<=ResponseTime4<=ResponseTime5<=ResponseTime6<=Late Response Time を入力します。
Voice	[Call Signal Monitoring] チェックボックスをオンにし、NAM がサポートする値ごとに MOS 品質範囲を入力します。
RTP Filter	[RTP Stream Monitoring] チェックボックスをオンにし、送信元および宛先の IPv4/IPv6 アドレスとマスクを使用してフィルタを入力します。
Aggregation Interval	短期および長期の間隔として最小値を入力します。

[Network Analysis Module] > [System]

次の表で、[Configuration] > [Templates] > [Features and Technologies] > [Network Analysis Module] > [System] の各フィールドについて説明します。

表 2-117　[NAM Analysis Module] > [System]

フィールド	説明
DNS Parameters	ドメイン名と DNS サーバの IP アドレスを入力します。
SNMP Agent	読み取り/書き込みアクセス許可を持つ SNMP コミュニティを作成します。
System Time	[Synchronize System Time With NTP] チェックボックスをオンにし、プライマリ NTP サーバ名/IP アドレス（IPv4 または IPv6）、セカンダリ NTP サーバ名/IP アドレス（IPv4 または IPv6）、およびタイム ゾーンを入力します。
Email Setting	[Mail] チェックボックスをオンにし、外部メール サーバおよびメール アラームの送信先（メール ID）を入力します。
Web Data Publication	[Web Data Publication] チェックボックスをオンにし、アクセス リストの IP アドレスまたは許可する必要があるサブネットを入力します。
SNMP Trap	SNMP トラップの IP アドレスおよび UDP ポートとともにコミュニティの詳細情報を入力します。

注　システム テンプレートのジョブ ステータスは、NAM デバイスに発生した変更以外の NAM3 の表示の障害時に展開します。

[Wireless Configuration] フィールドの説明

次に、[Design] > [Configuration] > [Wireless Configuration] にあるページの各フィールドについて説明します。

- FlexConnect Parameters
- Lightweight AP Configuration Templates
- Switch Location Configuration Template
- Autonomous AP Migration Templates
- Controller Configuration Groups
- [Plug and Play Profile] フィールドの説明

FlexConnect Parameters

次の表で、[Configuration] > [Network] > [Network Devices] を選択し、[Device Type] > [Wireless Controller] を選択し、コントローラのデバイス名をクリックしてから [FlexConnect] を選択した場合の [FlexConnect] の各フィールドについて説明します。

表 2-118　[Wireless Controller] > [FlexConnect Parameters]

フィールド	説明
[General] タブ	
Template Name	このコントローラに適用されるテンプレートの名前。
Primary Radius	ドロップダウン リストから、コントローラ上に存在するプライマリ RADIUS 認証サーバを選択します。選択または設定した RADIUS 認証サーバが、バージョン 7.4 以下のコントローラにない場合は、テンプレートは失敗します。 Prime Infrastructure の FlexConnect RADIUS サーバ設定を適用する前に、コントローラ上で RADIUS サーバ設定を行う必要があります。
Secondary Radius	ドロップダウン リストから、コントローラ上に存在するセカンダリ RADIUS 認証サーバを選択します。RADIUS 認証サーバがコントローラ上にない場合は、Prime Infrastructure で設定した RADIUS サーバは適用されません。
[FlexConnect AP] タブ	
Ethernet MAC	FlexConnect グループに適用するには、このチェックボックスをオンにします。 AP のイーサネット MAC アドレスは、同じコントローラ上の複数の FlexConnect グループには存在できません。AP イーサネット MAC が別の FlexConnect グループにすでに存在する場合、その AP イーサネット MAC を FlexConnect グループに設定することは、コントローラでは許可されていません。
Add AP	クリックして、既存の FlexConnect グループに追加の FlexConnect AP（Prime Infrastructure に存在しているもの）を追加します。[Add AP] をクリックした場合、この FlexConnect グループの一部であるアクセス ポイントのみがリストされます。 FlexConnect グループのローカル認証を有効にするには、[FlexConnect Configuration] タブをクリックします。[General] タブで、[Primary RADIUS Server] パラメータと [Secondary RADIUS Server] パラメータが [None] に設定されていることを確認します。
LEAP	FlexConnect アクセス ポイントで LEAP を使用してクライアントを認証できるようにする場合に選択します。
EAP-FAST	FlexConnect アクセス ポイントで EAP-FAST を使用してクライアントを認証できるようにする場合に選択します。EAP-FAST キーを指定するとともに、EAP-FAST キーを確認する必要があります。
Protected Access Credentials (PACs)	• 手動の PAC プロビジョニングを使用するには、[EAP=FAST Key] テキスト ボックスに、PAC の暗号化と暗号化解除に使用するキーを入力します。キーは 32 桁の 16 進数文字である必要があります。 • PAC プロビジョニング中に PAC のないクライアントに自動的に PAC を送信できるようにするには、[Ignore Server Key] チェックボックスをオンにします。
EAP-FAST Authority ID	EAP-FAST サーバの権限識別子を入力します。識別子は 32 桁の 16 進数文字である必要があります。
EAP-FAST Authority Info	テキスト形式の EAP-FAST サーバの権限識別子を入力します。32 桁までの 16 進数文字を入力できます。
EAP-FAST PAC Timeout	編集テキスト ボックスに PAC が表示される秒数を入力することによって、PAC タイムアウト値を指定します。有効な範囲は 2 ～ 4095 秒です。

表 2-118　[Wireless Controller] > [FlexConnect Parameters]（続き）

フィールド	説明
[Image Upgrade] タブ	
FlexConnect AP Upgrade	FlexConnect アクセス ポイントをアップグレードする場合に、このオプションを選択します。
Slave Maximum Retry Count	スレーブが FlexConnect グループ内のマスターからのダウンロード開始を試行する最大回数を指定する場合に、このオプションを選択します。このオプションは、[FlexConnect AP Upgrade] チェックボックスをオンにした場合のみ使用できます。 [General] タブで [FlexConnect AP Upgrade] チェックボックスが有効になっている場合に限り、アクセス ポイントをマスター アクセス ポイントとして追加できます。

Lightweight AP Configuration Templates

[Lightweight AP Configuration Templates] > [Template Basic]

次の表で、[Configuration] > [Templates] > [Lightweight Access Points] にある [Template Basic] タブの各フィールドについて説明します。

表 2-119　[Lightweight AP Configuration Templates] > [Template Basic]

フィールド	説明
Template Name	Lightweight AP 設定テンプレートの名前。
Description	Lightweight AP 設定テンプレートの説明。

[Lightweight AP Configuration Templates] > [AP Parameters]

次の表で、[Configuration] > [Templates] > [Lightweight Access Points] にある [AP Parameters] タブの各フィールドについて説明します。

表 2-120　[Lightweight AP Configuration Templates] > [AP Parameters]

フィールド	説明
General	
Location	[Location] テキスト ボックスに位置を入力します。
Admin Status	[Admin and Enabled] チェックボックスをオンにして、管理ステータスを有効にします。 エネルギーを節約するために、アクセス ポイントを作業時間以外の指定された時間にオフにすることができます。[Enabled] チェックボックスを選択することで、アクセス ポイントを有効にしたり、無効にしたりできます。

表 2-120　[Lightweight AP Configuration Templates] > [AP Parameters]（続き）

フィールド	説明
AP Mode	ドロップダウン リストから、次のいずれかを選択します。 • [Local]：デフォルト。 • [Monitor]：モニタ モードのみ。 [Monitor] をオンにして、Cisco Adaptive wIPS のアクセス ポイント テンプレートを有効にします。[Monitor] を選択した場合、[Enhanced WIPS Engine] チェックボックスおよび [Enabled] チェックボックスをオンにします。[AP Monitor Mode Optimization] チェックボックスをオンにして、[AP Monitor Mode Optimization] ドロップダウン リストから [WIPS] を選択します。 • [FlexConnect]：Cisco 1030 IEEE 802.11a/b/g/n リモート エッジ Lightweight アクセス ポイントで使用される Cisco 1030 リモート エッジ Lightweight アクセス ポイント（REAP）。 OfficeExtend アクセス ポイントを設定するには、[FlexConnect] を選択する必要があります。AP モードが [FlexConnect] の場合、[OfficeExtend AP] および [Least Latency Controller Join] を有効にするオプションなど、[FlexConnect] 設定オプションが表示されます。 • [Rogue Detector]：不正アクセス ポイントをモニタしますが、不正アクセス ポイントを送信したり、封じ込め処理をすることはありません。 • [Bridge] • [Sniffer]：アクセス ポイントは、所定のチャネルで無線を「スニファ」します。アクセス ポイントは、そのチャネル上のクライアントからのすべてのパケットを取得し、AiroPeek（IEEE 802.11 無線 LAN のパケット アナライザ）を実行するリモート マシンに転送します。これには、タイムスタンプ、信号強度、パケット サイズなどの情報が含まれます。動作モードとして [Sniffer] を選択する場合、AP/無線テンプレートの [802.11b/g/n Parameters] または [802.11a/n Parameters] タブでチャネルとサーバ IP アドレスの入力を要求されます。 スニファ機能は、データ パケットのデコードをサポートする、サードパーティ製のネットワーク分析ソフトウェアである AiroPeek を実行する場合だけ有効になります。AiroPeek の詳細については、http://www.wildpackets.com を参照してください。 • [SE-Connect]：このモードでは、CleanAir 対応のアクセス ポイントをすべてのモニタ対象チャネルでの干渉検出に広く使用できます。IDS スキャンや Wi-Fi などのその他の機能はすべて一時停止されます。 このオプションは、アクセス ポイントが CleanAir 対応の場合のみ表示されます。 AP モードを変更すると、アクセス ポイントがリブートします。
AP Sub Mode	ドロップダウン リストからオプションを選択します。
Enhanced wIPS Engine	[Enhanced wIPS Engine] および [Enabled] チェックボックスをオンにして有効にします。
AP Height (feet)	アクセス ポイントの高さ（フィート）をテキスト ボックスに入力します。
Mirror Mode	ミラー モードを有効にするには、[Enable] チェックボックスをオンにします。
Country Code	適切な国コードをドロップダウン リストから選択します。
Stats Collection Interval	状態収集間隔をテキスト ボックスに入力します。
Cisco Discovery Protocol	Cisco Discovery Protocol を有効にするには、[Enable] チェックボックスをオンにします。

表 2-120　[Lightweight AP Configuration Templates] > [AP Parameters]（続き）

フィールド	説明
AP Failover Priority	ドロップダウン リストから [Low]、[Medium]、[High] または [Critical] を選択して、アクセス ポイント フェールオーバー優先度を示します。デフォルトの優先度は [Low] です。
Pre-Standard 802.3af switches	Pre-Standard 802.3af switches
Antenna Band Mode	Antenna Band Mode
Domain Name	ドメイン名はスタティック IP がある AP でのみ設定できます。
Server IP Address	ドメイン名 サーバ IP はスタティック IP がある AP でのみ設定できます。
暗号化	暗号化を有効にするには、[Encryption] チェックボックスを選択します。
Rogue Detection	不正検出を有効にするには、チェックボックスを選択します。
SSH Access	SSH アクセスを有効にするには、[SSH Access] チェックボックスを選択します。
Telnet Access	Telnet アクセスを有効にするには、[Telnet Access] チェックボックスをオンにします。
Link Latency	コントローラでリンク遅延を設定して、アクセス ポイントおよびコントローラの間のリンクを計測できます。 **注**　リンク遅延は、接続モードの FlexConnect アクセス ポイントでのみサポートされます。スタンドアロン モードの FlexConnect アクセス ポイントはサポートされません。
TCP Adjust MSS	[TCP Adjust MSS] チェックボックスをオンにして、TCP を有効にして MSS を調整します。
VLAN Tagging	VLAN タギングは、バージョン 7.3.1.26 以降のコントローラでのみサポートされています。VLAN タギングのモードまたは値を変更した場合は、アクセス ポイントが再起動されます。VLAN タギングは、AP がブリッジ モードの場合は有効にできません。VLAN タギングを有効にすると、ネイティブ VLAN ID は無視されます。
AP Group Name	AP グループの名前。
Reboot AP	何らかの更新を行った後のアクセス ポイントの再起動を有効にするには、このチェックボックスをオンにします。
Power Injector Configuration	
Power Injector State	有効にすると、コントローラに直接移動せずに、Prime Infrastructure を介してパワー インジェクタ設定を操作できます。[Enable Power Injector State] を選択した場合、パワー インジェクタ オプションが表示されます。
Power Injector Selection	ドロップダウン リストから [Installed] または [Override] を選択します。
Injector Switch MAC Address	インジェクタ スイッチの MAC アドレスを入力します。
Global Username Password Configuration	
Override Global Username Password	グローバル ユーザ名およびパスワードの上書きを有効にするには、チェックボックスをオンにします。新しいアクセス ポイント ユーザ名およびパスワードを、該当するテキスト ボックスに入力し確認します。

表 2-120　[Lightweight AP Configuration Templates] > [AP Parameters]（続き）

フィールド	説明
Supplicant Credentials Configuration	
Override Supplicant Credentials	このアクセス ポイントがコントローラから認証ユーザ名およびパスワードを継承しないようにするには、[Override Supplicant Credentials] チェックボックスをオンにします。デフォルト値はオフです。[Override Supplicant Credentials] オプションは、コントローラ リリース 6.0 以降でサポートされます。 [Username]、[Password]、および [Confirm Password] テキスト ボックスに、このアクセス ポイントに割り当てる一意のユーザ名およびパスワードを入力します。
AP Retransmit Configuration	
AP Retransmit Count	AP 再送信回数を入力します。[AP Retransmit Count] のデフォルト値は 5 で、範囲は 3 ～ 8 です。
AP Retransmit Interval (secs)	AP 再送信間隔を入力します。[AP Retransmit Interval] のデフォルト値は 3 です。指定できる範囲は 2 ～ 5 です。
Controller Configuration	
Controllers Configuration	プライマリ、セカンダリおよびターシャリ コントローラ名のドロップダウン リストを有効にするには、このチェックボックスをオンにします。 • [Primary, Secondary, and Tertiary Controller Name]:プライマリ/セカンダリ/ターシャリ コントローラ名。 • [Primary, Secondary, and Tertiary Controller IP]:プライマリ、セカンダリ、ターシャリ コントローラ IP は、コントローラの管理 IP です。
Venue Configuration	Venue Group Venue Type Secondary Venue Name Language

[Lightweight AP Configuration Templates] > [Mesh]

次の表で、[Configuration] > [Templates] > [Lightweight Access Points] にある [Mesh] タブの各フィールドについて説明します。

表 2-121　[Lightweight AP Configuration Templates] > [Mesh]

フィールド	説明
Bridge Group Name	ブリッジ グループ名(最大 10 文字)をテキスト ボックスに入力します。 **注**　ブリッジ グループは、メッシュ アクセス ポイントを論理的にグループ化して、同一チャネル上の 2 つのネットワークが互いに通信しないようにするために使用されます。メッシュ アクセス ポイントが通信するためには、同じブリッジ グループ名が付いている必要があります。複数の RAP を使用する設定の場合は、ある RAP から別の RAP へフェールオーバーできるように、すべての RAP に同じブリッジ グループ名が付いていることを確認してください。
Data Rate (Mbps)	ドロップダウン リストから、バックホール インターフェイスのデータ レートを選択します。使用可能なデータ レートは、バックホール インターフェイスによって指示されます。デフォルトのレートは 18 Mbps です。 **注**　このデータ レートは、メッシュ アクセス ポイント間で共有され、メッシュ ネットワーク全体に対して固定されます。展開したメッシュ ネットワーク ソリューションに対してデータ レートを変更しないでください。
Ethernet Bridge	[Ethernet Bridging] ドロップダウン リストから、メッシュ アクセス ポイントの Ethernet ブリッジングを有効にします。
Role	メッシュ アクセス ポイントのロールをドロップダウン リストから選択します([MAP] または [RAP])。デフォルトの設定は MAP です。 メッシュ ネットワークのアクセス ポイントは、ルート アクセス ポイント(RAP)またはメッシュ アクセス ポイント(MAP)として機能します。
Ethernet Interfaces area	このグループ ボックスには、インターフェイス名、モード、VLAN ID、およびトランク ID などの情報が表示されます。適切なインターフェイスを選択し、そのモードを指定します。

[Lightweight AP Configuration Templates] > [802.11a/n/ac]

次の表で、[Configuration] > [Templates] > [Lightweight Access Points] にある [802.11a/n/ac] タブの各フィールドについて説明します。

表 2-122　[Lightweight AP Configuration Templates] > [802.11a/n/ac]

フィールド	説明
802.11a parameters	適用する必要がある 802.11a/n パラメータのチェックボックスをオンにします。 • Channel Assignment • Channel Width • Admin Status • Antenna Mode • Antenna Diversity • Antenna Type and Antenna Name • Antenna Name
802.11ac parameters	適用する必要がある 802.11ac パラメータのチェックボックスをオンにします。802.11ac パラメータは、11ac モジュールにのみ適用できます。 • Channel Width • Admin Status
Power Assignment	適切な電力レベルを選択するには、[Power Assignment] チェックボックスをオンにします。
Antenna Selection	11n アンテナ選択パラメータを選択するには、[Antenna Selection] チェックボックスをオンにします。
CleanAir	CleanAir 機能を有効にするには、[CleanAir] チェックボックスをオンにします。CleanAir は、CleanAir 対応 AP 用の WLC リリース 7.0 以降でサポートされています。

[Lightweight AP Configuration Templates] > [802.11a SubBand]

次の表で、[Configuration] > [Templates] > [Lightweight Access Points] にある [802.11a SubBand] タブの各フィールドについて説明します。[802.11a SubBand] サブでは、適用する必要がある 802.11a Sub Band オプション（4.9 または 5.8 パラメータ）を選択します。[SubBand] オプションは、フィールド左側のチェックボックスがオンでない限り無効です。

表 2-123　[Lightweight AP Configuration Templates] > [802.11a SubBand]

フィールド	説明
Admin Status	管理権限を有効にする場合は、[Admin Status] チェックボックスをオンにします。
Channel Assignment	チェックボックスをオンにして、該当するチャネルをドロップダウン リストから選択します。 **注**　チャネル番号は、その無線でサポートされているチャネル一覧に対して検証されます。
Power Assignment	チェックボックスをオンにして、該当する電力レベルをドロップダウン リストから選択します。 **注**　電力レベルは、その無線でサポートされている電力レベル一覧に対して検証されます。
WLAN Override	チェックボックスをオンにして、[Disable] または [Enable] をドロップダウン リストから選択します。 **注**　WLAN の上書きについての変更を有効にするためには、このアクセス ポイントをリセットする必要があります。
Antenna Type	外部アンテナまたは内部アンテナかを示します。
Antenna Name	[Antenna Type] チェックボックスをオンにして、適切なアンテナ名をドロップダウン リストから選択します。

[Lightweight AP Configuration Templates] > [802.11b/g/n]

次の表で、[Configuration] > [Templates] > [Lightweight Access Points] にある [802.11b/g/n] タブの各フィールドについて説明します。

表 2-124　[Lightweight AP Configuration Templates] > [802.11b/g/n]

フィールド	説明
Channel Assignment	グローバル割り当て方式を選択するか、カスタムを選択してチャネルを指定します。
Admin Status	管理権限を有効にする場合はオンにします。
Antenna Mode	アンテナ モードを選択します。
Antenna Diversity	[Enabled] または [Disabled] を選択します。アンテナ ダイバーシティは、適切なアンテナを選択するためにアクセス ポイントが 2 つの統合アンテナ ポートから無線信号をサンプリングすることをいいます。
Antenna Name	[Antenna Type] チェックボックスをオンにして、適切なアンテナ名をドロップダウン リストから選択します。
Power Assignment	グローバル割り当て方式を選択するか、カスタムを選択して電力割り当てを指定します。
Tracking Optimized Monitor Mode	[Enable] を選択します。
11n Antenna Selection	[11n Antenna Selection] チェックボックスをオンにして、適切なアンテナをリストから選択します。
CleanAir	ClearAir を有効にするには、このチェックボックスをオンにします。

[Lightweight AP Configuration Templates] > [CDP]

次の表で、[Configuration] > [Templates] > [Lightweight Access Points] にある [CDP] タブの各フィールドについて説明します。

表 2-125　[Lightweight AP Configuration Templates] > [CDP]

フィールド	説明
Cisco Discovery Protocol on Ethernet Interfaces	CDP を有効にするイーサネット インターフェイス スロットのチェックボックスをオンにします。
Cisco Discovery Protocol on Radio Interfaces	CDP を有効にする無線インターフェイス スロットのチェックボックスをオンにします。

[Lightweight AP Configuration Templates] > [FlexConnect]

次の表で、[Configuration] > [Templates] > [Lightweight Access Points] にある [FlexConnect] タブの各フィールドについて説明します。

表 2-126　[Lightweight AP Configuration Templates] > [FlexConnect]

フィールド	説明
FlexConnect Configuration	FlexConnect 設定(VLAN サポート、ネイティブ VLAN ID およびプロファイル名 VLAN マッピングなど)を有効にするには、このチェックボックスをオンにします。 **注**　これらのオプションは、FlexConnect モードのアクセス ポイントだけで使用できます。
OfficeExtend	デフォルトは [Enabled] です。 このチェックボックスを選択解除すると、単にこのアクセス ポイントの OfficeExtend モードが無効になります。アクセス ポイントの設定すべてが取り消されることはありません。アクセス ポイント設定をクリアし、工場出荷時設定に戻す場合、アクセス ポイント詳細ページ下部の [Clear Config] をクリックします。アクセス ポイント パーソナル SSID だけをクリアする場合、アクセス ポイント詳細ページ下部の [Reset Personal SSID] をクリックします。 [Enable for the OfficeExtend AP] を選択した場合、いくつかの設定が自動的に変更されます。たとえば、暗号化およびリンク遅延が有効になり、不正検出、SSH アクセス、Telnet アクセスが無効になります。 OfficeExtend アクセス ポイントを有効にする場合、少なくとも 1 つのプライマリ、セカンダリ、ターシャリ コントローラ(名前および IP アドレスを含む)を設定する必要があります。
Least Latency Controller Join	有効にした場合は、アクセス ポイントは、プライオリティ順序検索(プライマリ、セカンダリ、ターシャリ コントローラ)から、遅延測定値が最善(最短遅延)のコントローラの検索に切り替えます。遅延が最短のコントローラが、最善のパフォーマンスを提供します。 アクセス ポイントは、コントローラを初めて追加したときにこの検索を一度のみ実行します。接続後は、プライマリ、セカンダリおよびターシャリの遅延測定を再計算して、遅延測定が変わったかどうかを確認されることはありません。
VLAN Support	VLAN サポートを有効にするには、このチェックボックスをオンにします。
Native VLAN ID	有効なネイティブ VLAN ID の範囲は 1 ～ 4094 です。モードを REAP に変更するときに、アクセス ポイントがまだ REAP モードでない場合、他のすべての REAP パラメータはそのアクセス ポイントに適用されません。
WLAN VLAN Mapping	WLAN VLAN マッピング(WLAN プロファイル名と VLAN ID のマッピングなど)を有効にするには、[WLAN VLAN Mapping] チェックボックスをオンにします。
Web Auth ACL Mapping	VLAN ID ACL マッピングを有効にするには、[VLAN ID ACL Mapping] チェックボックスをオンにします。VLAN ID を入力して、ドロップダウン リスト ボックスから [Ingress and Egress ACLs] を選択して、指定 VLAN ID にマッピングします。
Policy ACL Mapping	ポリシー ACL マッピングを有効にするには、[Policy ACL Mapping] チェックボックスをオンにします。
Local Split ACL Mapping	ローカル スプリット ACL マッピングを有効にするには、[Local Split ACL Mapping] チェックボックスをオンにします。

[Lightweight AP Configuration Templates] > [Schedule]

次の表で、[Configure] > [Lightweight AP Configuration Templates] にある [Schedule] ページの各フィールドについて説明します。

表 2-127　[Lightweight AP Configuration Templates] > [Schedule]

フィールド	説明
Start Time	スケジュールした時間にテンプレートの展開を設定し、開始できます。 [Now]:テンプレートを直ちに展開します。 [Date]:テキスト ボックスに日付を入力するか、カレンダーのアイコンを使用して開始日を選択します。
Recurrence	[none]、[hourly]、[daily] または [weekly] から選択して、スケジュールの発生頻度を指定します。 テンプレートは [AP Selection] タブまたは [Schedule] タブを使用して展開できます。

Switch Location Configuration Template

次の表で、[Design] > [Wireless Configuration] > [Switch Location Configuration] にある [Template Detail] の各フィールドについて説明します。

表 2-128　[Design] > [Wireless Configuration] > [Switch Location Configuration]

フィールド	説明
Map Location	
Campus	スイッチまたはスイッチ ポートのマップ位置のキャンパスを選択します。
Building	スイッチまたはスイッチ ポートのマップ位置のビルディングを選択します。
Floor	スイッチまたはスイッチ ポートのマップ位置のフロアを選択します。
Import	選択したキャンパス、ビルディングおよびフロアの Civic 情報をインポートします。
ELIN and Civic Location	
ELIN	緊急ロケーション識別番号。
[Civic Address] タブ	スイッチ/スイッチ ポートで使用できる Civic 住所情報。
[Advanced] タブ	スイッチ/スイッチ ポート位置に関する詳細情報。
NMSP	スイッチの NMSP を有効または無効にするには、このチェックボックスをオンまたはオフにします。

Autonomous AP Migration Templates

次の表で、[Design] > [Configuration] > [Wireless Configuration] > [Autonomous AP Migration Templates] にある [Template Detail] の各フィールドについて説明します。

表 2-129　[Autonomous AP Migration Template] ページ

フィールド	説明
Name	テンプレート名。
Description	テンプレートの説明
AP Count	AP の数。
Schedule Run	スケジュールされた実行時刻。
Status	次のいずれかを示します。 • [Not initiated]:テンプレートの移行が未開始ですが、スケジュールされた時刻に開始します。 • [Disabled]:テンプレートが無効で、スケジュールされた時刻に実行しません。これは、Autonomous アクセス ポイントを選択せずに作成された場合のテンプレートのデフォルト状態です。 • [Expired]:テンプレートは、スケジュールされた時刻に実行しませんでした(Prime Infrastructure サーバがダウンしていた可能性があります)。 • [Enabled]:テンプレートの移行が未開始ですが、スケジュールされた時刻に開始します。 • [In progress]:テンプレートは、現在、選択した Autonomous アクセス ポイントを CAPWAP に変換しています。 • [Success]:テンプレートは、Autonomous アクセス ポイントの CAPWAP への移行を正常に完了しました。 • [Failure]:テンプレートは、選択された Autonomous アクセス ポイントから CAPWAP へのすべての移行に失敗しました。[View Migration Status] ページを使用して、失敗の詳細ステータスを確認できます。 • [Partial Success]:テンプレートは、選択された Autonomous アクセス ポイントから CAPWAP へのサブセットの移行に失敗しました。[View Migration Status] ページを使用して、失敗の詳細ステータスを確認できます。

[Autonomous AP Migration Templates] > [Add Template]

次の表で、[Design] > [Configuration] > [Wireless Configuration] > [Autonomous AP Migration Templates] にある [Template Detail] の各フィールドについて説明します。

表 2-130　Autonomous AP Migration Templates

フィールド	説明
Upgrade Options	
DHCP Support	変換後にすべてのアクセス ポイントが DHCP サーバから IP を取得したことを確認します。

表 2-130　Autonomous AP Migration Templates（続き）

フィールド	説明
Retain AP HostName	このアクセス ポイントに対して同じホスト名を保持できます。 AP から CAPWAP に初めて移行する場合だけ、ホスト名が CAPWAP で維持されます。AP のアップグレードを複数回行っている場合、ホスト名が維持されない場合があります。Autonomous アクセス ポイントのホスト名が 32 文字を超えると、CAPWAP アクセス ポイントのホスト名は default に設定されます。 アクセス ポイントを 12.3(11)JA、12.3(11)JA1、12.3(11)JA2、12.3(11)JA3 Autonomous イメージから LWAPP にアップグレードする場合、変換されるアクセス ポイントは、スタティック IP アドレス、ネットマスク、ホスト名およびデフォルト ゲートウェイを維持しない場合があります。
Migrate over WANLink	アクセス ポイントで実行される CLI コマンドのデフォルトのタイムアウトを延長します。 このオプションを有効にした場合、env_vars ファイルにリモート TFTP サーバ位置が保存されます。この情報は、アクセス ポイントにコピーされます。このオプションが選択されていない場合、Prime Infrastructure 内部 TFTP サーバを使用して、*env_vars* ファイルをアクセス ポイントにコピーします。
DNS Address	DNS アドレスを入力します。
Domain Name	ドメイン名を入力します。
Controller Details	
Controller IP	コントローラ IP アドレスを入力します。
AP Manager IP	アクセス ポイント マネージャ IP アドレスを入力することで、アクセス ポイントが接続するコントローラを指定します。 SSC 対応アクセス ポイントの場合、この IP アドレスは、コントローラ IP フィールドと同じにする必要があります。MIC 対応アクセス ポイントの場合、IP アドレスが一致する必要はありません。
User Name	ユーザ名を入力します。
Password	ユーザ名のパスワードを入力します。
TFTP Details	
TFTP Server IP	Prime Infrastructure サーバの IP アドレスを入力します。Prime Infrastructure は、インストールおよびセットアップ中に独自の TFTP および FTP サーバを提供します。
File Path	Prime Infrastructure 設定時に定義した TFTP ディレクトリを入力します。
File Name	Prime Infrastructure 設定時に TFTP ディレクトリで定義された CAPWAP 変換ファイルを入力します（例：c1240-rcvk9w8-tar.123-11JX1.tar）。
Schedule Details	
Apply Template	移行のテンプレートを適用するときのオプションを選択します。
Notification	通知を送信する受信者の電子メール アドレスを入力します。

Controller Configuration Groups

次に、[Design] > [Wireless Configuration] > [Wireless Configuration] > [Controller Configuration Groups] の各フィールドについて説明します。

- [Controller Configuration Groups] > [Add Config Group]（2-151 ページ）
- [Controller Configuration Groups] > [General]（2-151 ページ）
- [Controller Configuration Groups] > [Apply Schedule]（2-152 ページ）

[Controller Configuration Groups] > [Add Config Group]

次の表で、[Controller Configuration Groups] > [Add Config Group] にある [Template Detail] の各フィールドについて説明します。

表 2-131　[Wireless Configuration] > [Controller Configuration Groups]

フィールド	説明
Group Name	すべてのグループを通じて、グループ名は一意である必要があります。
Templates	Prime Infrastructure で作成されたその他のテンプレートを、設定グループに割り当てることができます。同じ WLAN テンプレートを、1 つ以上の設定グループに割り当てできます。次の中から選択します。 • [Select and add later]：後でテンプレートを追加します。 • [Copy templates from a controller]：別のコントローラからテンプレートをコピーします。現在のコントローラ一覧からコントローラを選択して、それに適用されているテンプレートを新しい設定グループにコピーします。テンプレートだけがコピーされます。 **注**　無線テンプレートを使用する場合、テンプレートの順序が重要になります。たとえば、テンプレート リストに無線テンプレートが含まれ、無線パラメータを適用する前に無線ネットワークを無効にする必要がある場合、まず無線ネットワークを無効にするテンプレートをテンプレートに追加する必要があります。

[Controller Configuration Groups] > [General]

次の表で、[Controller Configuration Groups] > [General] にある [Template Detail] の各フィールドについて説明します。

表 2-132　[Wireless Configuration] > [Controller Configuration Groups] > [General]

フィールド	説明
Enable Background Audit	選択した場合は、このグループに含まれるすべてのテンプレートが、ネットワークとコントローラの監査中にコントローラに対して監査されます。 **注**　このオプションを有効にするには、[Administration] > [System] > [Audit] で表示されるテンプレート ベースの監査オプションを設定します。
Enable Enforcement	選択した場合は、何らかの矛盾が見つかったときに監査中にテンプレートが自動的に適用されます。 **注**　このオプションを有効にするには、[Administration] > [System] > [Audit] で表示されるテンプレート ベースの監査オプションを設定します。

表 2-132　[Wireless Configuration] > [Controller Configuration Groups] > [General]（続き）

フィールド	説明
Enable Mobility Group	選択した場合は、モビリティ グループ名がグループ内のすべてのコントローラに適用されます。
Mobility Group Name	グループ内のすべてのコントローラにプッシュされる名前。このフィールドを使用して、グループ名を変更することもできます。 **注**　コントローラを複数の設定グループに含めることができます。
Last Modified On	設定グループを最後に変更した日付と時刻。
Last Applied On	最後に変更を適用した日付と時刻。

[Controller Configuration Groups] > [Apply Schedule]

次の表で、[Controller Configuration Groups] > [Apply Schedule] にある [Template Detail] の各フィールドについて説明します。

表 2-133　[Wireless Configuration] > [Controller Config Groups] > [Apply Schedule]

フィールド	説明
Apply	**注**　[Schedule] オプションが有効になっていない場合にのみ、このオプションを使用できます。 [Apply] をクリックして、モビリティ グループ、モビリティ メンバー、およびテンプレートのプロビジョニングを、設定グループのすべてのコントローラに対して開始します。適用後には、このページを離れたり、Prime Infrastructure からログアウトすることができます。プロセスは継続され、後でこのページに戻りレポートを表示できます。 **注**　プロビジョニングの適用時は、その他の設定グループの機能は実行しないでください。 [Recent Apply Report] ページにレポートが表示されます。コントローラのそれぞれに正常に適用されたモビリティ グループ、モビリティ メンバー、またはテンプレートが表示されます。
Schedule	[Schedule] オプションを有効にすると、[Apply] オプションは無効になります。
Start Date Start Time	開始日時を入力し、[Schedule] をクリックします。

[Compliance] フィールドの説明

次に、[Compliance] フィールドについて説明します。

- [Configuration] > [Compliance] > [Policies]
- [Configuration] > [Compliance] > [Jobs]
- [Configuration] > [Compliance] > [Jobs]
- [Plug and Play Profile] フィールドの説明

[Configuration] > [Compliance] > [Policies]

表 2-134　[Configuration] > [Compliance] > [Policies] > [New Rule Fields]

フィールド	説明
Rule Information	
このセクションに入力するすべての情報はフリー テキストであり、条件や後続の違反には影響しません。	
Rule Title	ルールの名前を入力します。
Description	簡単な説明を入力します。
Impact	ルールが生成する違反の影響に関する簡単なメモを入力します。
Suggested Fix	特定のポリシーに対してルールを選択するかどうかの判断に役立つ、修正についての簡単な説明を入力します。この説明は、[Rule Selector] ペインのルールを確認するときに表示されます。
Platform Selection	
Available Platforms	条件を実行する必要があるプラットフォームをオンにします。シスコ デバイスを選択した場合は、リストに指定されたすべてのシスコ プラットフォームが含められます。このセクションでオンにしたプラットフォームは監査ジョブの無視回数に影響します。たとえば、[Available Platforms] ペインで選択されていないデバイスを含めて、範囲内のすべてのデバイスでルールを実行した場合、そのようなデバイスは監査されず、無視回数に対してマークされます。
Rule Inputs	
New Rule Input	新しいルールに情報を追加するには、[New] をクリックします。このペインで作成する情報は、[Policy Profile] ペインに反映されます。選択したルールのルール情報を指定する必要があります。例えば、IP アドレスに情報を作成できます。このルールを実行するユーザがルールに固有の IP アドレスを入力したり、そのアドレスを特定のプロファイルに追加したりできます。必要な次の詳細情報を入力します。 識別子については、自身の識別子を入力するか、[Generate] ボタンをクリックして、タイトルに基づく識別子を生成します。 [Data Type] フィールドで選択したオプションに基づいて、次のフィールドが表示されます。 • [Is List of Values]：ルール情報に関連付ける複数の値を追加するには、このチェックボックスをオンにします。値の追加、編集、削除ができる表が表示されます。また、デフォルト値を設定することもできます。 • [Accept Multiple Values]：監査時に複数の値を指定する場合は、このチェックボックスをオンにします。これは、実行タイプのルール情報の場合にのみ適用されます。 • [Min Value]：ルール情報の最小整数値を入力します。これは、整数データ型の場合にのみ適用されます。 • [Max Value]：ルール情報の最大整数値を入力します。これは、整数データ型の場合にのみ適用されます。 • [Default Value]：ルール情報のデフォルト値を入力します。このフィールドに入力する値の形式は、[Data Type] フィールドで選択したデータ型によって異なります。例えば、データ型として [Integer] を選択した場合は、入力できるのは整数値のみです。 • [Max Length]：ルール情報に適用される最大長を入力します。 • [Val RegExp]：実行または修正に使用される有効な正規表現を入力します。

表 2-134　[Configuration] > [Compliance] > [Policies] > [New Rule Fields]（続き）

フィールド	説明
Conditions and Actions	
New Conditions and Actions	新しいルールの条件およびアクションを作成するには、[New] をクリックします。
[New Conditions and Actions—Conditions Details] タブ	
Condition Scope Details	• [Condition Scope]：次のいずれかから条件の範囲を選択します。 – [Configuration]：完全な実行コンフィギュレーションをオンにします。 – [Device Command Outputs]：show コマンドの出力を確認します。 – [Device Properties]：実行中の設定ではなく、デバイスのプロパティに対して確認を行います。 – [Previously Matched Blocks]：以前の条件で定義されているブロックに対して条件を実行します。このオプションで条件を実行するには、以前の条件で [Parse as Block] オプションをオンにしている必要があります。このオプションは、ルールの最初の条件に設定できません。 • [Device Property]：次のデバイス プロパティのいずれかを選択します。 – Device Name – IP Address – OS Name – OS Version **注**　このオプションは、[Condition Scope] ドロップダウン リストの [Device Properties] を選択した場合にのみ、有効になります。 • [Show Commands]：選択したプラットフォームに適用される必須の show コマンドを選択します。また、監査を実行する必要がある show コマンドも入力できます。 **注**　このオプションは、[Condition Scope] ドロップダウン リストの [Device Command Outputs] を選択した場合にのみ、有効になります。
Block Options	
Parse as Blocks	このオプションをオンにすると、実行中の設定ファイル内の特定のブロックの条件（このセクションで定義）を実行できるようになります。このオプションは、[Condition Scope] オプションで [Configuration] を選択した場合の show コマンドのみを対象とします。
Block Start Expression	このフィールドは、[Parse as Blocks] オプションが有効になっている場合は必須です。正規表現を使用してください。ここでは、ルール情報と、Grep 出力を使用できます。
Block End Expression	このフィールドは任意です。デフォルトでは、最上位またはサブレベルのコマンドが開始されたときにブロックが終了します。これよりも前にブロックを中断する場合は、正規表現として値を入力します。

表 2-134　[Configuration] > [Compliance] > [Policies] > [New Rule Fields]（続き）

フィールド	説明
Rule Pass Criteria	必要に応じて、オプションをオンにします。各オプションは次のとおりです。 • [All Sub Blocks]:すべてのブロックが指定された条件を満たした場合にのみ、ルールは成功したとマークされます。 • [Any Sub Block]:サブ ブロックのいずれかが条件を満たしている場合でも、ルールを成功したとしてマークします。 • [Raise One Violation for Each Failing Instance]:このオプションを有効にした場合、[Job view] で指定した違反回数は、各ブロックで条件が違反を検出した回数だけ増加します。
Condition Match Criteria	
Operator	後続のフィールドで入力する値に基づいてオプションを選択します。
Operator Function	[Edit] をクリックします。[Select Operator Function] ページが表示されます。事前定義の関数を選択し、選択した事前定義の関数に基づいて関数のパラメータを入力します。 **注**　このフィールドは、[Operator] フィールドでオプションの [Execute a Function] を選択した場合にのみ使用できます。
Value	値には正規表現を使用してください。ここでは、ルール情報と、Grep 出力を使用できます。この変数は、grep して後続の条件に使用できます。例えば、<2.1> <2.2> などの <Condition.value number> 条件規則に従います。この数値識別子は、前にフィールドで選択された演算子の入力パラメータとして、次の条件から使用できます。
Rule Pass Criteria	必要に応じて、オプションをオンにします。各オプションは次のとおりです。 • [All Sub Blocks]:すべてのブロックが指定された条件を満たした場合にのみ、ルールは成功したとマークされます。 • [Any Sub Block]:サブ ブロックのいずれかが条件を満たしている場合でも、ルールを成功したとしてマークします。 • [Raise One Violation for Each Failing Instance]:このオプションを有効にした場合、[Job view] で指定した違反回数は、各ブロックで条件が違反を検出した回数だけ増加します。
[New Conditions and Actions—Action Details] タブ	
Select Action	コンプライアンス監査を違反を検出した時点で実行する必要があるアクションを次のうちから 1 つ選択します。 • [Continue]:条件を満たしている、または満たしていない場合に、このフィールドに指定された条件番号に基づいてルールが続行します。条件番号を指定しない場合は、ルールは次の条件までスキップします。 • [Does Not Raise a Violation]:違反を発生させずに、その後のルールの実行を停止します。 • [Raise a Violation]:違反を発生させ、その後のルールの実行を停止します。 • [Raise a Violation and Continue]:違反を発生させ、ルールの実行を継続します。
Condition Number	条件を満たしている場合、または満たしていない場合によってルールを続行する条件番号を指定します。現在の条件番号以下の条件番号は指定できません。このフィールドは、[Select Action] フィールドでオプションの [Continue] を選択した場合にのみ使用できます。[Condition Number] フィールドが空白の場合に、次の利用可能な条件を使用できます。

表 2-134　[Configuration] > [Compliance] > [Policies] > [New Rule Fields]（続き）

フィールド	説明
Violation Severity	違反を検出した場合に、コンプライアンス監査にフラグを設定する必要がある重大度を指定します。このフィールドは、[Select Action] フィールドでオプションの [Raise a Violation] を選択した場合にのみ使用できます。
Violation Message Type	次のメッセージ タイプのいずれかを選択します。 • [Default Violation Message]：修正不能（または手動介入が必要）と判断した場合に、このオプションを選択します。 • [User defined Violation Message]：コメントを入力し、違反を修正する CLI 修正を提供するには、このオプションを選択します。 このフィールドは、[Select Action] フィールドでオプションの [Raise a Violation] を選択した場合にのみ使用できます。
Violation Message	**注**　このフィールドは、[Violation Message Type] フィールドでユーザ定義の違反メッセージを選択した場合にのみ使用できます。 [Job View] ウィンドウに表示される違反メッセージを入力します。ここに、ルール情報を使用できます。
Fix CLI	**注**　このフィールドは、[Violation Message Type] フィールドでユーザ定義の違反メッセージを選択した場合にのみ使用できます。 デバイスが指定した条件を満たしていない場合に、関連する CLI 修正を入力します。**config t**、**configure**、およびその **exit** コマンドを入力しないでください。ここでは、ルール情報と、Grep 出力を使用できます。 **注**　**exit** コマンドはメインおよびサブレベル コマンドで使用できます。 次に、このフィールドに入力する CLI 修正の形式を示します。 • 実行タイプの入力の場合は、<Rule input ID> を入力します。 • 修正タイプの入力の場合は、^<Rule input ID>^ を入力します。 • Grep タイプの出力の場合は、<n.m> を入力します。ここで、n は条件番号、m は出力番号です。

[Configuration] > [Compliance] > [Jobs]

表 2-135 に、監査済み/監査なしのデバイス、コンプライアンス監査に選択したルール、コンプライアンスの状態、違反数、インスタンス数、最大重度、および無視数についての情報を示します。

表 2-135　[Configuration] > [Compliance] > [Jobs Details and Violations Summary Fields]

フィールド	説明
Audited/Non-Audited Devices	監査済みおよび監査なしのデバイスの数を表示します。デバイスの詳細については、監査済みおよび監査なしのデバイスのハイパーリンク回数をクリックします。監査済みデバイスのハイパーリンク回数をクリックすると、デバイス名と監査ステータスが表示されます。監査なしデバイスには、次の数が含まれます。 • ジョブのスケジュール中にユーザの対象範囲にあったが、その後に変更されたデバイス。ジョブ実行時にこれらのデバイスはユーザの対象範囲にはありませんでした。 • ジョブ実行時にダウンしていたか、または到達できなかったデバイス。 • IOS モードでなかった CPT デバイス。Compliance Manager に必要な実行コンフィギュレーションが含まれていないため、これらのデバイスは監査されません。 • サードパーティ デバイス。 • コンプライアンス サーバと同期していないデバイス。つまり、デバイスの要素タイプがコンプライアンス サーバで使用できません。
Selected Rules	ポリシー プロファイルが作成されたときにポリシーで選択されたルールの数。これは、ポリシーに定義されたルールの総数のサブセットの場合があります。
Compliance State	[Pass] または [Fail] が表示されます。すべてのデバイスについてのポリシー内のすべてのルールが、[Pass] を表示する状態を裏付ける必要があります。
Violation Count	これは、各ジョブ内で確認された、異なる違反（特定のポリシー、デバイスの数）の数を一覧表示します。例えば、特定のポリシーの違反が 100 のデバイスであった場合、違反の数は 1 のみです。
Instance Count	すべてのデバイスの違反数の概要。例えば、特定のポリシーの違反が 100 のデバイスであった場合、インスタンスの数は 100 になります。
Highest Severity	ポリシーを構成するさまざまなルールの最高重大度。最大（ルールの作成時点で特定）を示します。これは、それよりも重大度が低い項目を上書きします。
Ignore Count	これは、ルールに対して定義されたプラットフォームの範囲外のデバイスであるために無視されたルールの数を示します。

[Plug and Play Profile] フィールドの説明

次に、[Plug and Play profiles] の各フィールドについて説明します。

- [Configuration] > [Plug and Play] > [Profiles]
- [Configuration] > [Plug and Play] > [Profiles] > [Deploy]

[Configuration] > [Plug and Play] > [Profiles]

次の表で、[Configuration] > [Plug and Play] > [Profiles] の各フィールドについて説明します。

表 2-136　[Configuration] > [Plug and Play] > [Profiles]

フィールド	説明
Device Type	このプロファイルに使用できる新しいデバイスのタイプを選択します。 一括導入では、イメージと設定の同じセットを使う同じ導入プロファイルを複数デバイスで使用します。デバイス ID を指定して導入プロファイルを使用するには、[Device Type] は選択*しない*でください。
Bootstrap Template	ドロップダウン リストからブートストラップ CLI テンプレートを選択します。
Software Image Image Location	ソフトウェア イメージをドロップダウン リストから選択し、イメージを配信するデバイス上のフラッシュの位置を指定します。
Configuration Template	ドロップダウン リストから設定テンプレートを選択します。

[Configuration] > [Plug and Play] > [Profiles] > [Deploy]

次の表で、[Configuration] > [Plug and Play] > [Profiles] > [Deploy] の各フィールドについて説明します。

表 2-137　[Configuration] > [Plug and Play] > [Profiles] > [Deploy]

フィールド	説明
Device ID	CNS ID ベースの展開の場合、これはハードウェア シリアル ID またはデバイスの VUDI になります。
Bootstrap Template Properties	ゲスト アカウントのユーザ名とパスワード、説明、日時、および属性リストの名前を入力します。 [Configuration] > [Plug and Play] > [Profiles] で定義されたブートストラップ テンプレートがある場合にのみ、ブートストラップ テンプレートのプロパティがプロファイル パラメータに表示されます。ブートストラップ テンプレートに関連付けられたすべての管理対象変数が、[Bootstrap Template Properties] の下に表示されます。
Configuration Template Properties	[Configuration] > [Plug and Play] > [Profiles] で定義された設定テンプレートがある場合にのみ、設定テンプレートのプロパティがプロファイル パラメータに表示されます。設定テンプレートに関連付けられたすべての管理対象変数が [Configuration Template Properties] の下に表示されるため、ユーザはこれらの変数に値を入力し、[Apply] をクリックできます。
Image Properties	次の詳細情報を持つイメージがプロファイルに指定されている場合、イメージのプロパティが [Profile Parameters] に表示されます。 • Image location • Erase Flash • Continue on Image Failure • Activate Image

表 2-137　[Configuration] > [Plug and Play] > [Profiles] > [Deploy]（続き）

フィールド	説明
Device Management Parameters	IP アドレスを入力します。CNS ベースの展開では、IP アドレスが指定されていない場合、Prime Infrastructure Plug and Play ゲートウェイによって指定された IP アドレスが、デバイスを Prime Infrastructure のデバイス インベントリに追加するために使用されます。 ネットワークがファイアウォールと NAT によって保護されている場合、Prime Infrastructure Plug and Play ゲートウェイ サーバによって指定された IP アドレスがデバイスの実際の IP アドレスでない場合があります。Prime Infrastructure によって管理される必要がある NAT の背後に複数のデバイスがある場合、管理者はそのデバイスの IP アドレスを手動で入力できます。 **注**　Cisco Prime Infrastructure はデバイスに関するデバイス管理パラメータを提供*しません*。デバイス管理パラメータは、イメージおよび CLI 設定が適用された後にデバイスを管理するために、Prime Infrastructure によって使用されます。すべての設定が、プロファイルの設定テンプレートを介してのみ実行されます。 **注**　デバイスに管理パラメータを設定する場合は、プラグ アンド プレイ プロファイルに含まれている設定テンプレートに追加します（*『Cisco Prime Infrastructure 3.0 User Guide』*の「Creating Plug and Play Profiles（プラグ アンド プレイ プロファイルの作成）」を参照してください）。
SNMP Parameters	バージョン、タイムアウト、再試行回数、コミュニティ名を入力します。
CLI Parameters	ドロップダウン リストからプロトコルを選択し、ユーザ名、パスワード、確認パスワード、有効化パスワード、確認有効化パスワード、タイムアウトを入力します。

[Mobility Services] フィールドの説明

次に、Mobility Service Engine を設計するフィールドについて説明します。

Mobility Services Engines

次のセクションでは、[Design] > [Mobility Services] > [Mobility Services Engine] にあるページの各フィールドについて説明します。

[Mobility Services Engines] > [Select a command] > [Add Location Server]

次の表で、[Design] > [Mobility Services] > [Mobility Services Engines] > [Select a command] > [Add Location Server] にある [Template Detai]l フィールドについて説明します。

表 2-138　[Add Location Server]

フィールド	説明
Device Name	Mobility Services Engine のデバイス名
IP Address	Mobility Services Engine の IP アドレス。
Contact Name	Mobility Services Engine の管理者。
User Name	デフォルトのユーザ名は admin です。これは、MSE に対して設定されている Prime Infrastructure 通信ユーザ名です。
Password	デフォルトのパスワードは admin です。これは、MSE に対して設定されている Prime Infrastructure の通信パスワードです。
Port	Mobility Services Engine デバイスのポート番号。
HTTPS	有効に設定した場合、Prime Infrastructure とロケーション サーバ間の通信には HTTPS が使用されます。

[Mobility Services Engines] > [Select a command] > [Add Mobility Services Engine]

次の表で、[Design] > [Mobility Services] > [Mobility Services Engine] > [Select a command] > [Add a Mobility Services Engine] にある [Template Detai]l フィールドについて説明します。

表 2-139　Mobility Services Engine の追加

フィールド	説明
Device Name	Mobility Services Engine のユーザ割り当て名。
IP Address	Mobility Services Engine の IP アドレス。
Contact Name	Mobility Services Engine の管理者。
Username	デフォルトのユーザ名は admin です。これは、MSE に対して設定されている Prime Infrastructure 通信ユーザ名です。
Password	デフォルトのパスワードは admin です。これは、MSE に対して設定されている Prime Infrastructure の通信パスワードです。
HTTP	有効に設定されている場合、Prime Infrastructure と Mobility Services Engine 間の通信に HTTP が使用されます。デフォルトでは、Prime Infrastructure は MSE との通信に HTTPS を使用します。

Mobility Services Engines Database Synchronization

次の表で、[Design] > [Mobility Services] > [Mobility Services Engine] > [Select a command] > [Add Mobility Services Engine] にある [Template Detai]l フィールドについて説明します。

表 2-140　Mobility Services Engine の追加

フィールド	説明
Device Name	Mobility Services Engine のユーザ割り当て名。
IP Address	Mobility Services Engine の IP アドレス。
Contact Name	Mobility Services Engine の管理者。
Username	デフォルトのユーザ名は admin です。これは、MSE に対して設定されている Prime Infrastructure 通信ユーザ名です。
Password	デフォルトのパスワードは admin です。これは、MSE に対して設定されている Prime Infrastructure 通信パスワードです。
HTTP	有効に設定されている場合、Prime Infrastructure と Mobility Services Engine 間の通信に HTTP が使用されます。デフォルトでは、Prime Infrastructure は MSE との通信に HTTPS を使用します。

ハイ アベイラビリティ

次の表で、[Design] > [Mobility Services] > [High Availability] にある [Template Detail] フィールドについて説明します。

表 2-141　ハイ アベイラビリティの設定

フィールド	説明
Device Name	プライマリ MSE とペアにするセカンダリ デバイスの名前。
IP Address	セカンダリ MSE のヘルス モニタ IP アドレスであるセカンダリ IP アドレス。
Contact Name	Mobility Services Engine の管理者。
Failover Type	フェールオーバー タイプを指定します。[Manual] または [Automatic] のいずれかを選択できます。10 秒後にシステムがフェールオーバーします。セカンダリ サーバは、プライマリ サーバからの次のハートビートを最大 10 秒間待機します。10 秒以内にハートビートを受信しないと、失敗が宣言されます。
Failback Type	フェールバック タイプを指定します。[Manual] または [Automatic] のいずれかになります。
Long Failover Wait	長時間のフェイルオーバー待機時間を秒単位で指定します。10 秒後にシステムがフェールオーバーします。最大フェールオーバー待機時間は 2 秒です。

スイッチの設定

次に、スイッチを構成するフィールドについて説明します。

- [Configure] > [Switches]
- [Configure] > [Switches] > [IP Address]
- [Configure]> [Switches] > [Add Switches]

[Configure] > [Switches]

次の表で、[Switches] ページのフィールドについて説明します。

表 2-142　スイッチの表示

フィールド	説明
Management IP Address	スイッチの IP アドレス。詳細を取得するには、スイッチの IP アドレスをクリックします。詳細については、「Viewing Switch Details（スイッチ詳細情報の表示）」（4-3 ページ）を参照してください。
Device Name	スイッチ名。
Device Type	スイッチのタイプ。
Reachability Status	スイッチが到達可能な場合は [Reachable]、スイッチが到達不能な場合は [Unreachable] を示します。
Inventory Collection Status	最後のインベントリ収集のステータス。可能な値は、[OK]、[Partial]、[Failed]、[NA]（SPT 専用スイッチの場合）、または [In Progress] です。
Inventory Status Detail	最新のインベントリ収集のステータスを指定します。インベントリ収集が正常に行われなかった場合は、失敗の考えられる理由がリストされます。

表 2-142　スイッチの表示（続き）

フィールド	説明
Last Inventory Collection Date	インベントリが収集された最後の日付が表示されます。
Creation Time	スイッチが Prime Infrastructure に追加された日付と時刻。
License Status	スイッチのライセンス ステータスを示します。これは、[Full Support] または [SPT only] です。

[Configure] > [Switches] > [IP Address]

次の表で、スイッチの詳細情報を表示している間に表示される概要情報の各フィールドについて説明します。

表 2-143　[Configure] > [Switches Summary Information]

General Parameters	
IP Address	スイッチの IP アドレス。
Device Name	スイッチ名。
Last Inventory Collection Date	最後のインベントリ収集の日付と時刻。
Inventory Collection Status	最後のインベントリ収集のステータス。可能な値は、[OK]、[Partial]、または [Failed] です。
Software Version	スイッチで実行されているソフトウェアのバージョン。
Location	スイッチの場所。
Contact	スイッチの担当者名。
Reachability Status	スイッチが到達可能な場合は [Reachable]、スイッチが到達不能な場合は [Unreachable] を示します。
SNMP Parameters	
Version	SNMP バージョン番号、これは、[v1]、[v2c]、または [v3] です。SNMP v3 で設定されたスイッチのスイッチ ポート トレーシングを正常に実行するには、該当する VLAN のコンテキストをスイッチで設定する必要があります。
Retries	プロセスが成功せずに停止するまでに許可される再試行値（秒単位）。
Timeout	プロセスがタイムアウトになるまでに許可される時間（秒単位）を示します。有効な範囲は 2 ～ 90 秒です。デフォルトは 10 秒です。
[Version] ドロップダウン リストで [v3] を選択した場合は、次のフィールドが表示されます。	
User Name	ユーザ名。
Auth.Type	認証タイプは、[None]、[HMAC-SHA]、または [HMAC-HD5] です。
Auth.Password	認証パスワード。
Privacy Type	プライバシー タイプは、[None]、[CBC-DES]、または [CFB-AES-128] です。
Privacy Password	プライバシー パスワード。
Community	[v1] または [v2c] を選択した場合は、このフィールドは SNMP コミュニティ ストリングを示します。

表 2-143　[Configure] > [Switches Summary Information]（続き）

General Parameters	
Telnet/SSH Parameters	
Protocol	使用されるプロトコル。
User Name	[Username]。
Password	パスワード。
Confirm Password	パスワードを再度入力して確認します。
Enable Password	有効化パスワード。
Confirm Password	パスワードを再度入力して確認します。
Timeout	タイムアウト値（秒単位）です。

[Configure]> [Switches] > [Add Switches]

次の表で、[Adding Switches] ページの各フィールドについて説明します。

表 2-144　スイッチの追加

フィールド	説明
General Parameters	
Add Format Type	次を選択します。 • [Device Info]：イーサネット スイッチの IP アドレスをカンマで区切って手動で入力します。 • [CSV File]：複数のスイッチの IP アドレスが含まれている CSV ファイルをインポートします。テキスト ボックスに CSV ファイルのパスを入力するか、[Browse] をクリックして、コンピュータで CSV ファイルにナビゲートします。
IP Addresses	[Device Info] を選択した場合は、イーサネット スイッチの IP アドレスをカンマで区切って入力します。
License Level	次を選択します。 • **[Full]** • [SPT only]：スイッチ ポート トレーシング サポートのみを指定します。
SNMP Parameters 書き込みアクセスに対応する SNMP パラメータ（使用できる場合）を入力します。読み取り専用アクセス パラメータを入力すると、スイッチは追加されますが、Prime Infrastructure は設定を変更できません。	
Version	SNMP バージョン番号を入力します。これは、[v1]、[v2c]、または [v3] です。SNMP v3 で設定されたスイッチのスイッチ ポート トレーシングを正常に実行するには、該当する VLAN のコンテキストをスイッチで設定する必要があります。
Retries	プロセスが成功せずに停止するまでに許可される再試行値（秒単位）を入力します。
SNMP Timeout (in secs)	SNMP タイムアウト値（秒単位）を入力します。
[Version] ドロップダウン リストで [v1] または [v2c] を選択した場合は、[Community] フィールドが表示されます。	
Community	SNMP コミュニティ ストリングを入力します。
[Version] ドロップダウン リストで [v3] を選択した場合は、次のフィールドが表示されます。	
Username	ユーザ名を入力します。

表 2-144　スイッチの追加（続き）

フィールド	説明
Auth.Type	[None]、[HMAC-SHA]、または [HMAC-HD5] の認証タイプを入力します。
Auth.Password	認証パスワードを入力します。
Privacy Type	[None]、[CBC-DES]、または [CFB-AES-128] のプライバシー タイプを入力します。
Privacy Password	プライバシー パスワードを入力します。
Telnet/SSH Parameters	
Protocol	プロトコルを選択します。
User Name	ユーザ名を入力します。
Password	パスワードを入力します。
Confirm Password	パスワードを再度入力して確認します。
Enable Password	有効化パスワードを入力します。
Confirm Password	有効化パスワードを再度入力して確認します。
Timeout (in secs)	タイムアウト値(秒単位)を入力します。

[CSV File] フィールド

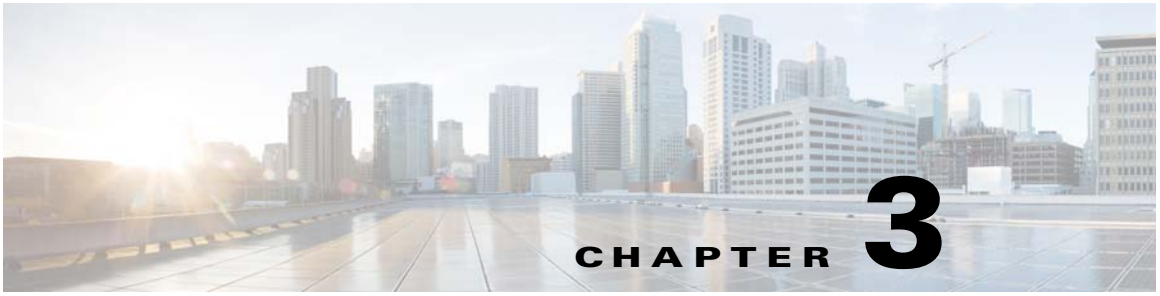
次の表で、[CSV] ファイルの各フィールドについて説明します。

表 2-145　[CSV] ファイルのフィールド

フィールド	説明
ip_address	IP アドレス
network_mask	ネットワーク マスク
snmp_version	SNMP クレデンシャル バージョン。v1、v2、または v3 です。
snmp_community	SNMP コミュニティ(v2 では必須)。
snmpv2_community	SNMP V2 コミュニティ。
snmpv3_user_name	SNMP V3 ユーザ名(v3 では必須)。
snmpv3_auth_type	SNMP V3 認証タイプ。None、HMAC-MD5、または HMAC-SHA です(v3 では必須)。
snmpv3_auth_password	SNMP V3 認証パスワード(v3 では必須)。
snmpv3_privacy_type	SNMP V3 プライバシー タイプ。None、DES、または CFB-AES-128 です(v3 では必須)。
snmpv3_privacy_password	SNMP V3 プライバシー パスワード(v3 では必須)。
snmp_retries	SNMP の再試行回数
snmp_timeout	SNMP のタイムアウト
protocol	telnet、ssh2
telnet_username	設定されている場合、スイッチおよび AP のユーザ名(設定されている場合は必須)。
telnet_password	スイッチと AP のパスワード(必須)

表 2-145　[CSV] ファイルのフィールド（続き）

フィールド	説明
enable_password	指定されたパスワードを有効にします
telnet_timeout	telnet のタイムアウト時間



[Inventory] ページのフィールド リファレンス

ここでは、Cisco Prime Infrastructure リリース 2.1 の [Inventory] タブにあるフィールドについて説明します。

NAT44 Rules

次に、[Inventory] > [Device Management] > [Network Devices] > [Configuration] > [Security] > [NAT] > [NAT44 Rules] にあるフィールドについて説明します。

- [Add NAT Rule] > [Static Rule]（ 3-1 ページ）
- [Add NAT Rule] > [Dynamic NAT Rule]（ 3-2 ページ）
- [Add NAT Rule] > [Dynamic PAT Rule]（ 3-3 ページ）

[Add NAT Rule] > [Static Rule]

次の表で、[Operate] > [Device Work Center] > [Configuration] > [Security] > [NAT] > [NAT44 Rules] > [Add NAT Rule] > [Static Rule] の要素について説明します。

表 3-1　[Add NAT Rule] > [Static Rule]

要素	説明
Direction	方向を入力します。Cisco Prime Infrastructure リリース 2.1 は受信から発信への方向のみをサポートします。
VRF	NAT 変換プロセスが実行される Virtual Routing and Forwarding（VRF）を入力します。
Source A	有効な IPv4 アドレスを入力します。有効な IPv4 アドレスは、ピリオド（.）で区切られた 4 つのオクテットから構成されます。 • [Source A] を定義した場合は、[Source B] も定義する必要があります。 • [Source A] を定義した場合は、[Destination A] はデフォルトで [Any] になります。
Destination A	有効な IPv4 アドレスを入力します。有効な IPv4 アドレスは、ピリオド（.）で区切られた 4 つのオクテットから構成されます。 • [Destination A] を定義した場合は、[Destination B] も定義する必要があります。 • [Destination A] を定義した場合は、[Source A] はデフォルトで [Any] になります。
Translation	スタティック変換のタイプを選択します。

表 3-1　[Add NAT Rule] > [Static Rule]（続き）

要素	説明
Source B	有効な IPv4 アドレスを入力します。有効な IPv4 アドレスは、ピリオド(.)で区切られた 4 つのオクテットから構成されます。また、インターフェイスのリストからインターフェイスを選択することもできます。 • [Source B] を定義した場合は、[Source A] も定義する必要があります。 • [Source B] を定義した場合は、[Destination B] はデフォルトで [Any] になります。
Destination B	有効な IPv4 アドレスを入力します。有効な IPv4 アドレスは、ピリオド(.)で区切られた 4 つのオクテットから構成されます。 • [Destination B] を定義した場合は、[Destination A] も定義する必要があります。 • [Destination B] を定義した場合は、[Source A] および [Source B] はデフォルトで [Any] になります。
Options	スタティック タイプの高度なオプションを入力します。次を設定します。 • 組み込み IP アドレス(ペイロードなし)を無視するには、[Ignore Embedded IP Address] チェックボックスをオンにします。 • ポート変換を有効にするには [Enable Port Translation] チェックボックスをオンにし、次を定義します。 – TCP または UDP – 元のポート – Translated Port

[Add NAT Rule] > [Dynamic NAT Rule]

次の表で、[Inventory] > [Device Management] > [Network Devices] > [Configuration] > [Security] > [NAT] > [NAT44 Rules] > [Add NAT Rule] > [Dynamic NAT Rule] の要素について説明します。

表 3-2　[Add NAT Rule] > [Dynamic NAT] ページ

要素	説明
Direction	方向を入力します。Cisco Prime Infrastructure リリース 2.1 は受信から発信への方向のみをサポートします。
VRF	NAT 変換プロセスが実行される VRF を入力します。
Source A	リストから ACL 名を選択します。 • [Source A] を定義した場合は、[Source B] も定義する必要があります。 • [Source A] を定義した場合は、[Destination A] はデフォルトで [Any] になります。
Destination A	リストから ACL 名を選択します。 • [Destination A] を定義した場合は、[Destination B] も定義する必要があります。 • [Destination A] を定義した場合は、[Source A] はデフォルトで [Any] になります。
Translation	ダイナミック NAT 変換のタイプを選択します。
Source B	ドロップダウン リストから NAT プールを選択します。

表 3-2　[Add NAT Rule] > [Dynamic NAT] ページ（続き）

要素	説明
Destination B	ドロップダウン リストから NAT プールを選択します。 • [Destination B] を定義した場合は、[Destination A] も定義する必要があります。 • [Destination B] を定義した場合は、[Source A] および [Source B] はデフォルトで [Any] になります。
Options	ダイナミック タイプの高度なオプションを入力します。 • 組み込み IP アドレス(ペイロードなし)を無視するには、[Ignore Embedded IP Address] チェックボックスをオンにします。 • ポート変換を有効にするには [Enable Port Translation] チェックボックスをオンにし、次を定義します。 – TCP または UDP – 元のポート – Translated Port **注**　このオプションは、Cisco サービス統合型ルータでのみサポートされています。

[Add NAT Rule] > [Dynamic PAT Rule]

次の表で、[Inventory] > [Device Management] > [Network Devices] > [Configuration] > [Security] > [NAT] > [NAT44 Rules] > [Add NAT Rule] > [Dynamic PAT Rule] の要素について説明します。

表 3-3　[Add NAT Rule] > [Dynamic PAT] ページ

要素	説明
Direction	方向を入力します。このリリースでは、インバウンドからアウトバウンドへの方向だけがサポートされています。
VRF	NAT 変換プロセスが実行される VRF を入力します。
Source A	リストから ACL 名を選択します。
Destination A	[Destination A] は定義できません。
Translation	ダイナミック PAT 変換のタイプを選択します。
Source B	リストから IP プール名を選択します。また、インターフェイスのリストからインターフェイスを選択することもできます。
Destination B	[Destination B] は定義できません。
Options	ダイナミック PAT の高度なオプションを入力します。組み込み IP アドレス(ペイロードなし)を無視するには、[Ignore Embedded IP Address] チェックボックスをオンにします。 **注**　このオプションは、Cisco ISR でのみサポートされています。

[Configuration] > [Security] > [Zone Based Firewall]

次の表で、[Inventory] > [Device Management] > [Network Devices] > [Configuration] > [Security] > [Zone Based Firewall] > [Policy Rule] にあるフィールドについて説明します。

表 3-4　[Zone Based Firewall] > [Policy Rule] ページ

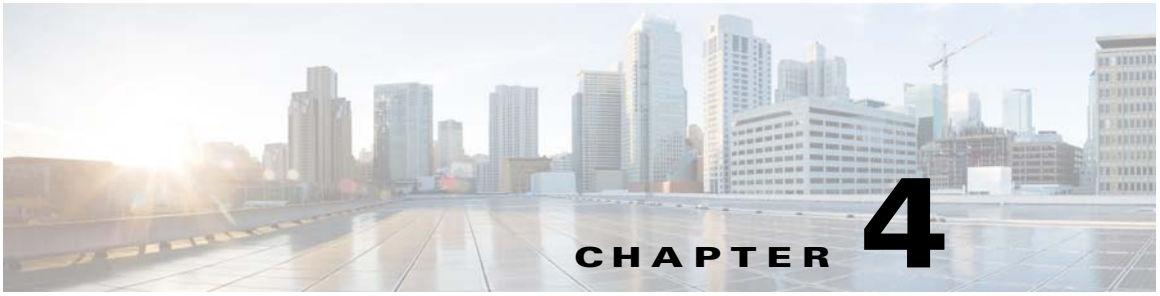
要素	説明
Name	(任意)ポリシー規則の名前を入力します。
Source Zone	トラフィックの起点となるゾーンの名前を入力します。
Destination Zone	トラフィックの宛先となるゾーンの名前を入力します。
Source	検査対象のデータの送信元 IP アドレスを入力します。有効なパラメータは次のとおりです。 • いずれか(Any) • IPv4 アドレスとサブネットの組み合わせ。
Destination	検査対象のデータの宛先 IP アドレスを入力します。有効なパラメータは次のとおりです。 • いずれか(Any) • IPv4 アドレスとサブネットの組み合わせ。
Service	検査対象のデータのサービス。有効なパラメータは次のとおりです。 • Services • Port Based Applications • TCP • UDP • ICMP
Action	規則条件に一致がある場合にトラフィック上で実行するアクションを選択します。次の場合に規則が一致します。 • トラフィックの送信元 IP アドレスが送信元規則条件と一致する。 • トラフィックの宛先 IP アドレスが宛先規則条件と一致し、トラフィックの検査対象サービスがサービス規則条件と一致する。 アクションのオプションは次のとおりです。 • Drop • Drop and Log • Inspect • Pass • Pass and Log
Advanced Options	[Action] オプションが [Inspect] に設定されているときに、ファイアウォール ルール パラメータマップ動作を設定するコンフィギュレーション パラメータを指定します。

[Service Container] > [Add]

次の表で、[Inventory] > [Device Management] > [Network Devices] > [Service Container] > [Add] にあるフィールドについて説明します。

表 3-5　[Operate] > [Device Work Center] > [Service Container] > [Add]

フィールド	説明
Select an Operation	コンテナを後でアクティブ化するか、または現在のインスタンス中にアクティブ化するかに応じて、[Install] または [Install and Activate] を選択します。
WAAS-XE IP Address/Mask	Cisco Wide Area Application Services（WAAS）- Cisco IOS XE コンテナの IP アドレスおよびマスクを入力します。
Router Virtual Interface IP/Mask	コンテナをインストールするルータ仮想インターフェイスの IP と マスクを入力します。
OVA	インストールする OVA イメージをリストから選択します。
Resource Profile	メモリに要件に応じて、リソース プロファイルをリストから選択します。
Service Container Name	サービス コンテナの名前を入力します。
Enable WAN Optimization on	WAN 最適化を開始するにはこのチェックボックスをオンにし、トラフィックのリダイレクションを開始するインターフェイスを選択します。



CHAPTER 4

[Maps] ページのフィールド リファレンス

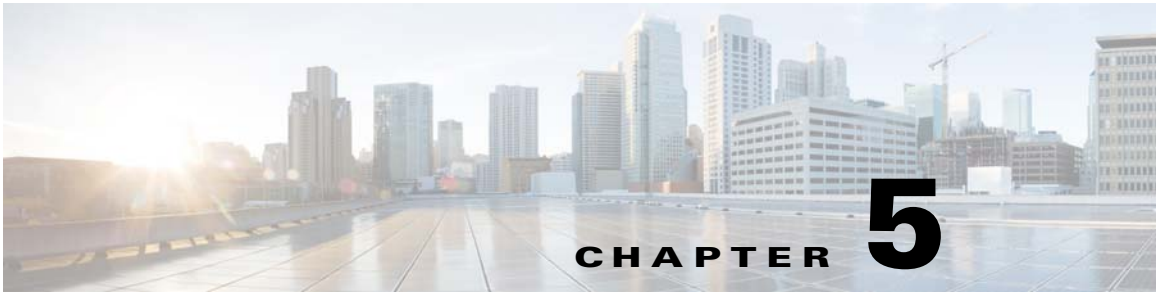
ここでは、Cisco Prime Infrastructure リリース 3.0 の [Maps] にあるページの各フィールドについて説明します。

[Wireless Maps] > [Site Maps] > [AP Mesh Info]

次の表で、[Maps] > [Wireless Maps] > [Site Maps] > [AP Mesh Info] ページの各フィールドについて説明します。

表 4-1　[Maps] > [Wireless Maps] > [Site Maps] > [AP Mesh Bridging Link Information]

フィールド	説明
Information fetched on	情報を集めた日時
Link SNR	リンクの Signal to Noise Ratio（SNR）
Link Type	階層化されたリンク関係
SNR Up	アップリンクの Signal to Noise Ratio（dB）
SNR Down	ダウンリンクの Signal to Noise Ratio（dB）
PER	リンクのパケット エラー率
Tx Parent Packets	親として動作する際のノードに対する TX パケット
Rx Parent Packets	親として動作する際のノードに対する RX パケット
Time of Last Hello	最後のハローの日時



CHAPTER 5

[Services] ページのフィールド リファレンス

ここでは、Cisco Prime Infrastructure リリース 3.0 の [Services] タブにあるフィールドについて説明します。

[Guest User] フィールドの説明

次に、[Services] > [Guest User] > [Add Guest User] > [New Controller Template] にあるフィールドについて説明します。

- [Guest User] > [Add Guest User] > [New Controller Template] > [General] タブ（5-1 ページ）
- [Guest User] > [Add Guest User] > [New Controller Template] > [Advanced] タブ（5-2 ページ）

[Guest User] > [Add Guest User] > [New Controller Template] > [General] タブ

次の表で、[Services] > [Guest User] > [Add Guest User] > [New Controller Template] > [General] ページにあるフィールドについて説明します。

表 5-1　[Guest User] > [Add Guest User] > [New Controller Template] > [General] タブ フィールドの説明

フィールド	説明
User Name	ゲスト ユーザ名を入力します。最大長は 24 文字です。
Generate Password	ゲスト ユーザ アカウントの作成スケジュールごとにユーザ名とパスワードを生成するには、このチェックボックスをオンにします。これを有効化すると、異なるパスワードが毎日（選択した日数分）支給されます。これを無効化すると（オフにする）、1 つのパスワードが選択した日数の間支給されます。オプションとして、スケジュールごとに新しいパスワードを生成できます。
Password	パスワードを入力します。パスワードには、次のような要求事項があります。 • パスワードには少なくとも 8 文字必要です。 • 小文字、大文字、数字、特殊文字の 4 種類の文字から 3 種類以上を使用してパスワードを作成する必要があります。
Confirm Password	[Password] フィールドに入力したパスワードを再入力します。
Description	ゲスト ユーザ テンプレートの説明を入力します。

表 5-1　[Guest User] > [Add Guest User] > [New Controller Template] > [General] タブ フィールドの説明（続き）

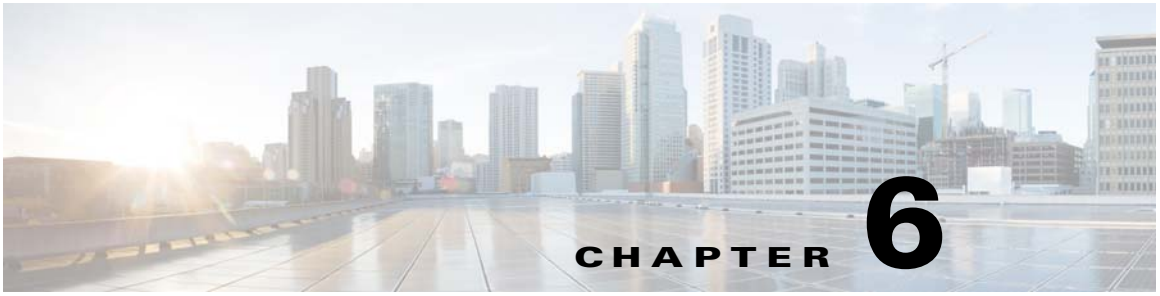
フィールド	説明
Disclaimer	デフォルトの免責事項テキスト。
Make this Disclaimer Default	免責事項テキストをこのゲスト ユーザ テンプレートのデフォルトとして設定するには、このチェックボックスをオンにします。

[Guest User] > [Add Guest User] > [New Controller Template] > [Advanced] タブ

次の表で、[Operate] > [Operational Tools] > [Wireless] > [Guest User] > [Add Guest User] > [New Controller Template] > [Advanced] にあるフィールドについて説明します。

表 5-2　[Guest User] > [Add Guest User] > [New Controller Template] > [Advanced タブ フィールドの説明

フィールド	説明
Import From File	ゲスト ユーザ テンプレートを一括してインポートするには、このチェックボックスをオンにします。
Profile	ゲスト ユーザが接続するプロファイルを選択します。
User Role	ドロップダウン リストから、ゲスト ユーザのユーザ ロールを選択します。ユーザ ロールは、管理者により事前に定義され、ゲストのアクセス（契約者、顧客、代理店、ベンダー、ビジターなど）にアソシエートされています。 ユーザ ロールを使用して、ネットワーク内の特定のユーザに割り当てられた帯域幅の量を管理します。
Life Time	ゲスト ユーザ アカウントをアクティブにしておく期間を次のオプションのいずれかを選択して定義します。 • [Limited]：時間および分のドロップダウン リストを使用して、ゲスト ユーザ アカウントをアクティブにする期間を選択します。[Limited] のデフォルト値は、1 日（8 時間）です。 • [Unlimited]：ゲスト アカウントの有効期限の日付はありません。 **注**　Cisco Catalyst 3850 スイッチ（Cisco IOS XE 3.2.1）および Cisco 5760 Wireless LAN コントローラのゲストアカウントの設定時に [Unlimited] を選択した場合は、ゲスト アカウントがアクティブになっている最大時間は 1 年になります。
Apply to	ドロップダウン リストから、次のいずれかを選択します。 • [Indoor Area]：キャンパス、ビルディング、フロア。 • [Outdoor Area]：キャンパス、屋外領域。 • [Controller List]：選択されたプロファイルが作成されたコントローラの一覧。 • [Config Groups]：Prime Infrastructure で設定した設定グループ名。



[Reports] ページのフィールド リファレンス

ここでは、Cisco Prime Infrastructure リリース 3.0 の [Reports] メニューにあるページの各フィールドについて説明します。

- [Report Launch Pad]
- [Report Results]
- [Scheduled Run Results]
- [Saved Report Templates]

[Report Launch Pad]

次に、[Reports] > [Report Launch Pad] にあるレポートの各フィールドについて説明します。

- [Report Launch Pad] > [Report Type] > [New]
- [Report Launch Pad] > [Report Type] > [New] > [Customize]

[Report Launch Pad] > [Report Type] > [New]

表 6-1　[Report Launch Pad] > [Report Type] > [New] フィールドの説明

フィールド	説明
Settings	
Create reports in current and each sub Virtual Domains	現在の仮想ドメイン内のみでなく、各サブ仮想ドメインについてもレポートを作成する場合は、このチェックボックスをオンにします。[View sub Virtual Domains] リンクをクリックすると、仮想ドメインの名前、電子メール アドレス、タイム ゾーンなどの仮想ドメインについての詳細情報が表示されます。 このチェックボックスをオンにしており、レポートがスケジュールされていない場合、レポート テンプレートは作成されてすべてのサブドメインに保存されますが、レポートは実行されません。[Create reports in current and sub Virtual Domains] チェックボックスをオンにし、レポートのスケジュールを設定すると、レポートはすべてのサブドメイン内でスケジュールされ、設定された時間に実行されます。 このチェックボックスをオンにした場合は、レポートのみを保存できます。その他すべてのオプション（[Run]、[Run And Save]、[Save And Report]、[Save And Email]）は、レポート詳細ページに表示されません。つまり、レポートは、サブドメインでだけ、作成と実行のスケジューリングが可能です。 レポートの作成時刻はシステムによって異なるため、レポートの作成とレポートの実行の間に十分な間隔を設けてください。
Report Title	レポート名を入力します。[Create reports in current and each sub Virtual Domains] チェックボックスをオンにした場合は、このレポートのタイトルの後ろに *_VirtualDomainName* が追加されます。*VirtualDomainName* はレポートが生成された仮想ドメインの名前です。
Report By	ドロップダウン リストから適切なカテゴリ別レポートを選択します。カテゴリはレポートごとに異なります。
Report Criteria	このフィールドを使用すると、前の [Report By] で行った選択に応じて、結果を分類できます。[Edit] をクリックして [Filter Criteria] ページを開き、必要なフィルタ基準を選択します。
Reporting Period	次のいずれかを実行します。 • [Select a time period] オプション ボタンをオンにし、ドロップダウンリストから時間を選択します。 • [From] オプション ボタンを選択して、開始日時と終了日時を入力します。テキスト ボックスに日付を入力するか、カレンダー アイコンをクリックして日付を選択できます。ドロップダウン リストから時間と分を選択します。
Schedule	
Scheduling	設定したスケジュールでレポートを実行するには、[Enable] チェックボックスをオンにします。
Export Format	レポート実行後にレポートの結果をエクスポートする場合のファイル形式として [CSV] または [PDF] を選択します。CSV ファイルおよび PDF ファイルのデフォルトの場所は、次のとおりです。 /ncs-ftp/reports/Inventory/*ReportTitleName_yyyymmdd_HHMMSS.csv* /ncs-ftp/reports/Inventory/*ReportTitleName_yyyymmdd_HHMMSS.pdf*

表 6-1　[Report Launch Pad] > [Report Type] > [New] フィールドの説明（続き）

フィールド	説明
Destination	宛先のタイプ（ファイルまたは電子メール）を選択します。該当するファイルの場所または電子メール アドレスを入力します。 [Create reports in current and each sub Virtual Domains] チェックボックスをオンにした場合は、[Email] ボタンではなく [Email to default Contact in each Virtual Domain] オプション ボタンが表示されます。[View Contacts] リンクをクリックすると、さまざまな仮想ドメインの電子メール ID を表示できます。 電子メール用のメール サーバの設定を行うには、左側のサイドバー メニューから [Administration] > [Settings]> [System Settings] を選択し、次に、[Mail Server Configuration] を選択して [Mail Server Configuration] ページを開きます。SMTP およびその他の必要な情報を入力します。 電子メール アドレスがサブ仮想ドメインに指定されていない場合は、現在の仮想ドメインに電子メール アドレスが指定されていれば、その電子メールアドレスが使用されます。
Start Date/Time	表示されたテキスト ボックスに日付を入力するか、カレンダー アイコンをクリックしてカレンダーを開き、日付を選択します。時間と分のドロップダウン リストから時刻を選択します。このデータに対するレポートの実行が、この日時に開始されます。 ここでいう時刻とは、Prime Infrastructure サーバの時間であり、ブラウザのローカル タイムではありません。 **注**　古い（たとえば、4 か月前の）レコードを使用してレポートを生成したり、1 週間分の集約テーブルに基づいてレポートを生成したりする場合、生成されたレポートには、1 週間に 1 つのエントリしか含まれません。 [Create reports in current and each sub Virtual Domains] チェックボックスをオンにした場合は、[Use Virtual Domain time zone] チェックボックスが表示されます。仮想ドメインのタイム ゾーンをレポートのタイム ゾーンとして使用する場合は、このチェックボックスをオンにします。さまざまな仮想ドメインのタイム ゾーンを表示するには、[View time zones] リンクをクリックします。
Recurrence	実行するレポートの頻度を次のオプションから選択します。 • [No Recurrence]：レポートは 1 度だけ実行されます（[Start Date/Time] で示した時間に実行）。 • [Hourly]：レポートは、[Entry] テキスト ボックスに入力する時間数で示す間隔で実行されます。 • [Daily]：レポートは、[Every] テキスト ボックスに入力する日数で示す間隔で実行されます。 • [Weekly]：レポートは、[Every] テキスト ボックスに入力する週数およびチェックボックスをオンにした曜日に実行されます。 • [Monthly]：レポートは、[Every] テキスト ボックスに入力する月数で示す間隔で実行されます。

[Report Launch Pad] > [Report Type] > [New] > [Customize]

表 6-2　[Report Launch Pad] > [Report Type] > [New] > [Customize Field Descriptions]

フィールド	説明
Custom Report Name	ドロップダウン リストからカスタマイズするレポートを選択します。 **注**　[Available data fields] 列と [Data fields to include] 列の見出しの選択項目は、選択したレポートにより異なる場合があります。
Available data fields/Data fields to include	強調表示されているフィールドを [Available data fields] 列と [Data fields to include] 列の間で移動するには、[Add] ボタンと [Remove] ボタンを使用します。 [Data fields to include] 列に青のフォントで表示されているフィールドは、[Custom Report Name] フィールドで選択したレポートの必須フィールドです。
[Change order] ボタン	結果テーブルの列の順序を決定するには、[Move Up] ボタンおよび [Move Down] ボタンを使用します。[Selected Columns] リストで上方の列見出しが、結果表の左方に表示されます。
Data field sorting	ソート設定を指定します([Ascending] または [Descending])。レポート データのソート方法を指定します。 ソート順序を指定できる 4 つのデータ フィールドを選択できます。[Sort by and Then by] ドロップダウン リストを使用して、ソート用の各データ フィールドを選択します。 分類する各データ フィールドについて、昇順で分類するか、降順で分類するかを選択します。 表形式のレポートのみソートできます(グラフおよび複合形式は不可)。ソートできるフィールドのみが [Data field sorting] ドロップダウン リストに表示されます。 [Create Custom Report] ページに表示される [Sortable fields] には、[Data fields to include] ペインにあるデータ フィールドだけでなく、ソート可能なすべてのフィールドがリストされます。レポートは、そのレポートに列が表示されていない場合も、選択したデータ フィールドに基づいて分類されます。

[Report Results]

ここでは、さまざまなタイプのレポートに表示される結果について説明します。表示される結果は、[Reports] > [Report Launch Pad] > [Report Type] > [New] > [Customize] > [Create Custom Report] ページで行ったカスタマイズによって異なります。

[Client Reports]

次に、[Client Reports] に表示されるフィールドについて説明します。

[Busiest Clients Report Results]

表 6-3　[Busiest Clients Report Results]フィールドの説明

フィールド	説明
Client MAC Address	クライアントの MAC アドレス。
IP Address	クライアントの IP アドレス。このフィールドには、IPv6 クライアントの場合は IPv6 アドレス、IPv4 およびデュアル スタック クライアントの場合は IPv4 アドレスが表示されます。
Protocol	802.11a/n または 802.11b/g/n。
Throughput	Mbps または kbps のいずれか。スループットが 0.1 kbps 未満の場合は、「<0.1 kbps」が表示されます。
Global Unique	IPv6 アドレスの集約グローバル ユニキャスト アドレス。このフィールドには、クライアントにグローバル固有 IPv6 アドレスが割り当てられている場合のみ値が入力されます。
Local Unique	IPv6 アドレスのローカル ユニキャスト アドレス。このフィールドには、クライアントにローカル固有 IPv6 アドレスが割り当てられている場合のみ値が入力されます。
Link Local	IPv6 アドレスのリンクローカル ユニキャスト アドレス。このフィールドには、クライアントにリンク ローカル IPv6 アドレスが割り当てられている場合のみ値が入力されます。
On Device	クライアントが配置されているデバイス。
Bytes sent (MB)	送受信する MB 単位のバイト数。 この値が 1,000,000,000 を超える場合は、値の末尾に G が追加されます（例：3.45 G）。この値が 1,000,000 を超え、1,000,000,000 未満の場合は、値の末尾に M が追加されます（例：456.8 M）。
Bytes received (MB)	
Packets sent	送受信されたパケット数（MB）。 この値が 1,000,000,000 を超える場合は、値の末尾に G が追加されます（例：3.45 G）。この値が 1,000,000 を超え、1,000,000,000 未満の場合は、値の末尾に M が追加されます（例：456.8 M）。
Packets received	

[Client Sessions Report Results]

表 6-4　[Client Sessions Report Results]フィールドの説明

フィールド	説明
Client Username	このクライアントのユーザ名。
IP Address	このクライアントの IP アドレス。
MAC Address	このクライアントの MAC アドレス。
Association Time	このクライアントが関連付けられた日時。
Access Point Name	このクライアントが割り当てられたアクセス ポイントの名前。
Map Location	クライアントが位置する建物、階、屋外の場所（該当する場合）。
SSID	このクライアントがアソシエートされた SSID。
Profile	このクライアントがアソシエートされたプロファイルの名前。
VLAN ID	VLAN 識別子。指定できる範囲は 1 ～ 4096 です。
Protocol	802.11a、802.11b、802.11g、802.11n_5GHz、または 802.11b_2.4GHz。

表 6-4　[Client Sessions Report Results]フィールドの説明（続き）

フィールド	説明
Policy Type	このクライアント セッションのセキュリティ ポリシーのタイプ。
Host Name	このクライアントが位置するマシンの DNS ホスト名。 Prime Infrastructure は、DNS ルックアップを実行して、クライアント IP アドレスからホスト名を解決します。IP アドレスとホスト名のマッピングが、DNS サーバで定義されている必要があります。デフォルトでは、ホスト名のルックアップは無効です。ホスト名のルックアップを有効にするには、[Administration] > [Settings] > [System] > [Settings] > [Clients] を使用します。
Global Unique	IPv6 アドレスの集約グローバル ユニキャスト アドレス。このフィールドには、クライアントにグローバル固有 IPv6 アドレスが割り当てられている場合のみ値が入力されます。
Local Unique	IPv6 アドレスのローカル ユニキャスト アドレス。このフィールドには、クライアントにローカル固有 IPv6 アドレスが割り当てられている場合のみ値が入力されます。
Link Local	IPv6 アドレスのリンクローカル ユニキャスト アドレス。このフィールドには、クライアントにリンクローカル IPv6 アドレスが割り当てられている場合のみ値が入力されます。
CCX	Cisco Client Extension のバージョン番号。
AP MAC Address	アクセス ポイントの MAC アドレス。
AP IP Address	アクセス ポイントの IP アドレス。
AP Radio	アクセス ポイントの無線タイプ。
Device IP Address	このクライアントがアソシエートされたデバイスの IP アドレス。
Device Port	このクライアントがアソシエートされたデバイスのポート番号。
Anchor Controller	モビリティ クライアントのアンカーまたは外部コントローラの IP アドレス（該当する場合）。
Association	このクライアント セッションで使用されたアソシエーション ID。
Disassociation Time	このクライアントの関連付けが解除された日時。
Authenticatio	このクライアントの認証方式。
Encryption Cypher	このクライアント セッションで使用された暗号化。
EAP Type	このクライアント セッションで使用された EAP タイプ。
Authentication Algorithm	このクライアント セッションで使用された EAP タイプ。
Web Security	このクライアント セッションで使用された Web セキュリティ。
Tx and Rx (bytes)	クライアント セッション中に送受信されたおおよそのバイト数。
SNR	このクライアント セッションの信号対雑音比。
RSSI	受信信号強度インジケータ（dBm 単位）。
Status	[Associated] または [disassociated]。
Reason	アソシエーション解除の理由。
E2E	バージョン番号または [Not Supported]。

[Client Traffic Stream Metrics Report Results]

表 6-5　[Client Traffic Stream Metrics Report Results]フィールドの説明

フィールド	説明
Time	アクセス ポイントから統計情報が収集された時刻。
Client MAC	クライアントの MAC アドレス。これには、直近の 90 秒間に評価されたクライアントのリストが表示されます。クライアントとしては、VoIP 電話、ラップトップ、PDA などがあり、測定値を収集しているアクセス ポイントに接続されたすべてのクライアントを示します。
QoS	WLAN に影響する可能性がある QoS 値(パケット遅延、パケット ジッター、パケット損失、ローミング時間)がモニタされます。アクセス ポイントおよびクライアントでメトリックを測定し、アクセス ポイントで計測結果を収集してこれらをコントローラに送信します。アクセス ポイントでは、90 秒ごとにコントローラのトラフィック ストリーム メトリック情報を更新し、クライアントごとに 10 分間分のデータが WLC に格納されます。Prime Infrastructure はこのデータをポーリングし、最後の 7 日間について保存します。
AP Name	このクライアントが関連付けられるアクセス ポイントの名前。
Radio Type	アクセス ポイントの無線タイプ。
Avg Queuing Delay (ms) (Downlink)	ダウンリンクの平均キューイング遅延(ミリ秒単位)。パケット キューイング遅延の平均は、音声キューを横断する音声パケットの平均遅延です。パケット キュー遅延は、パケットが送信のためにキューに入れられた時点から、パケットが正常に送信される時点まで測定されます。これには、必要に応じて再試行時間が含まれます。
Avg Queuing Delay (ms) (Uplink)	アップリンクの平均キューイング遅延(ミリ秒単位)。パケット キューイング遅延の平均は、音声キューを横断する音声パケットの平均遅延です。パケット キュー遅延は、パケットが送信のためにキューに入れられた時点から、パケットが正常に送信される時点まで測定されます。これには、必要に応じて再試行時間が含まれます。
% PLR (Downlink)	90 秒間にダウンリンク(アクセス ポイントからクライアント)で損失したパケットの割合。
% PLR (Uplink)	90 秒間にアップリンク(クライアントからアクセス ポイント)で損失したパケットの割合。
% Packets > 40ms Queuing Delay (Uplink)	40 ミリ秒を超えるキューイング遅延パケットの割合。
% Packets 20ms-40ms Queuing Delay (Uplink)	20 ～ 40 ミリ秒範囲でのキューイング遅延パケットの割合。
Roaming Delay	ローミング遅延(ミリ秒単位)。クライアントによって測定されるローミング遅延は、古いアクセス ポイントから最後のパケットを受信した時点から、ローミングが正常に行われた後で新しいアクセス ポイントから最初のパケットを受信した時点まで測定されます。

[Unique Clients and Users Report Results]

表 6-6　[Unique Clients and Users Report Results] のフィールド説明

フィールド	説明
Client User Summary	クライアント ユーザのサマリ情報を表示します。ここでは、次の項目について説明します。 • 重複を除いたクライアント数 • セッション数 • 重複を除いたユーザ数 • 重複を除いた AP 数 • AP ごとの平均ユーザ数 • AP ごとの平均クライアント数 • 合計セッション時間(時間) • 平均セッション時間(分) • ユーザごとの平均セッション時間 • クライアントごとの平均セッション時間(分)
Client Traffic Summary	クライアント トラフィックのサマリ情報を表示します。合計トラフィック数と合計クライアント数のレポートには、最大 15 日間の 1 時間当たりのデータが表示されます。ここでは、次の項目について説明します。 • 合計トラフィック数(MB) • 合計スループット(Mbps) • 総セッション数 • 合計クライアント数 • 重複を除いた合計ユーザ数 • 合計セッション時間(時間) • セッションごとの平均トラフィック(KB) • ユーザごとの平均トラフィック(KB) • クライアントごとの平均トラフィック(KB) • セッションごとの平均スループット(Kbps) • ユーザごとの平均スループット(Kbps) • クライアントごとの平均スループット(Kbps)

表 6-6　[Unique Clients and Users Report Results] のフィールド説明（続き）

フィールド	説明
Client Summary by Protocol	プロトコル別のクライアント サマリを表示します。ここでは、次の項目について説明します。 • プロトコル：802.11a、802.11b、802.11g, 802.11n_5GHz, or 802.11b_2.4GHz, 802.3, 802.11ac • セッション数 • クライアント数 • ユーザ数 • セッション時間（時間） • トラフィック（MB） • 最大セッション数 • クライアントの割合（%） • ユーザの割合（%） • セッション時間の割合（%） • トラフィックの割合（%）
Client Summary by Vendor	ベンダー別のクライアント サマリを表示します。ここでは、次の項目について説明します。 • ベンダー • セッション数 • クライアント数 • ユーザ数 • セッション時間（時間） • トラフィック（MB） • 最大セッション数 • クライアントの割合（%） • ユーザの割合（%） • セッション時間の割合（%） • トラフィックの割合（%）

[CCX Client Statistics Report Results]

表 6-7　[CCX Client Statistics Report Results]フィールドの説明

フィールド	説明
Client MAC Address	クライアントの MAC アドレス。
Transmitted Fragment Count	このカウンタは、正常に受信した MPDU データまたは管理タイプごとに増分されます。

表 6-7　[CCX Client Statistics Report Results]フィールドの説明（続き）

フィールド	説明
Multicast Transmitted	このカウンタは、正常に送信された MAC Service Data Unit（MSDU）の宛先 MAC アドレス中でマルチキャスト ビットが設定されている場合にのみ減少します。拡張サービス セット（ESS）のステーション（STA）として運用しているときは、これらのフレームはアクセス ポイントに送信されます。これは、すべての関連付けされた MAC プロトコル データ ユニット（MPDU）への確認応答を受信していることを示します。
Failed Count	このカウンタは、MSDU の送信が失敗した場合に、増分されます。
Retry Count	このカウンタは、1 回以上の再送信後に MSDU が正常に送信されたときに増分されます。
Multicast Retry Count	このカウンタは、複数回の再送信の後で MSDU が正常に送信された場合に増分されます。
Frame Duplicate Count	このカウンタは、Sequence Control フィールドで重複が示されているフレームを受信した場合に増分されます。
RTS Success Count	このカウンタは、RTS（送信要求）の応答として CTS（送信要求の解除）を受信したときに増分されます。
RTS Fail Count	このカウンタは、ready-to-send への応答として clear-to-send を受信しない場合に増分されます。
ACK Fail Count	このカウンタは、正常な ACK を受信しなかった場合に増分されます。
Received Fragment Count	長さが 64 オクテット（フレーミング ビットは除外するが、FCS オクテットは含む）未満の受信済みパケットの総数。
Multicast Received Frame Count	このカウンタは、マルチキャスト ビットが宛先 MAC アドレスに設定された MSDU を受信したときに増分されます。
FCS Error Count	このカウンタは、受信した MPDU でフレーム チェック シーケンス エラーが検出されたときに増分されます。
Transmitted Frame Count	このカウンタは、MSDU を正常に送信するたびに増分されます。

[Device Reports]

次に、[Device Reports] に表示されるフィールドについて説明します。

[AP Image Predownload Report Results]

表 6-8　[AP Image Predownload Report Results] フィールドの説明

フィールド	説明
AP Name	アクセス ポイントの名前。
Primary Image	AP にある現在のプライマリ イメージ。
Backup Image	AP にある現在のバックアップ イメージ。
Predownload Version	事前ダウンロード プロセスの一環としてコントローラから AP に現在ダウンロード中のイメージのバージョン。
Predownload Status	事前ダウンロード プロセスの一環であるイメージ ダウンロードの現在のステータス。

表 6-8　[AP Image Predownload Report Results] フィールドの説明（続き）

フィールド	説明
MAC Address	AP の MAC アドレス。
Controller IP Address	アクセス ポイントがアソシエートされたコントローラの IP アドレス。
Upgrade Role	アップグレード ロールの現在のステータス。これは次のいずれかになります。 • Master Central • Master Local • Slave Central • Slave Local • Unknown

[AP Profile Status Report Results]

表 6-9　[AP Profile Status Report Results] フィールドの説明

フィールド	説明
Time	AP プロファイル ステータスの収集日時。
AP Name	アクセス ポイントの名前。
AP MAC Address	アクセス ポイントの MAC アドレス。
Radio Type	802.11a/n または 802.11b/g/n。
Load	[Pass] または [Fail]。負荷レベルが閾値レベルを超えているかどうかを示します。
Noise	[Pass] または [Fail]。ノイズ レベルが閾値レベルを超えているかどうかを示します。
Interference	[Pass] または [Fail]。干渉レベルが閾値レベルを超えているかどうかを示します。
Coverage	[Pass] または [Fail]。カバレッジ レベルが閾値レベルを超えているかどうかを示します。
Controller Name	アクセス ポイントがアソシエートされたコントローラの名前。
Controller IP Address	アクセス ポイントがアソシエートされたコントローラの IP アドレス。

[Busiest APs Report Results]

表 6-10　[Busiest APs Report Results]フィールドの説明

フィールド	説明
AP Name	アクセス ポイントの名前。
Radio Type	802.11a/n または 802.11b/g/n。
Rx Utilization(%)	アクセス ポイント レシーバがパケットの操作でビジーになっている時間の割合。0 ～ 100 の数字で 0 ～ 1 の負荷を表します。
Tx Utilization(%)	アクセス ポイント トランスミッタがパケットの操作でビジーになっている時間の割合。0 ～ 100 の数字で 0 ～ 1 の負荷を表します。

表 6-10　[Busiest APs Report Results]フィールドの説明（続き）

フィールド	説明
Channel Utilization (%)	アクセス ポイント チャネルがパケットの操作でビジーになっている時間の割合。0 ～ 100 の数字で 0 ～ 1 の負荷を表します。
Controller Name	アクセス ポイントがアソシエートされたコントローラの名前。
Controller IP Address	アクセス ポイントがアソシエートされたコントローラの IP アドレス。
Map Location	アクセス ポイントが位置する建物、階、屋外の場所（該当する場合）。

[Scheduled Run Results]

次の表で、[Reports] > [Scheduled Run Results] ページの各フィールドについて説明します。

表 6-11　[Scheduled Run Results] のフィールドの説明

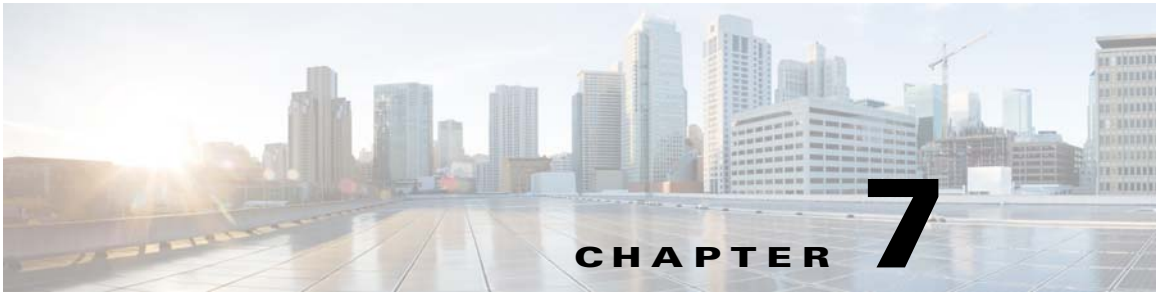
フィールド	説明
Report Category	ドロップダウン リストから適切なレポート カテゴリを選択するか、[All] を選択します。
Report Type	ドロップダウン リストから適切なレポート タイプを選択するか、[All] を選択します。レポート タイプの選択項目は、選択したレポート カテゴリに応じて変わります。
From/To	レポートの開始日（[From]）と終了日（[To]）をテキスト ボックスに入力するか、カレンダー アイコンをクリックして開始日と終了日を選択します。
Report Generation Method	次のオプションからいずれかのレポート生成方式を選択します。 • Scheduled • On-demand Export • On-demand Email

[Saved Report Templates]

次の表で、[Reports] > [Saved Report Templates] ページの各フィールドについて説明します。

表 6-12　[Saved Report Templates] のフィールドの説明

フィールド	説明
Report Category	ドロップダウン リストから適切なレポート カテゴリを選択するか、[All] を選択します。
Report Type	ドロップダウン リストから適切なレポート タイプを選択するか、[All] を選択します。レポート タイプの選択項目は、選択したレポート カテゴリに応じて変わります。
Scheduled	[All]、[Enabled]、[Disabled]、または [Expired] を選択して、スケジュールされたステータスによって [Saved Report Templates] リストをフィルタします。



[Administration] ページのフィールド リファレンス

この章では、Cisco Prime Infrastructure リリース 3.0 の **[Administration]** メニューにあるページの各フィールドについて説明します。

[アプライアンス]

次に [Administration] > [Settings] > [Appliance] ページの内容について説明します。

- [Appliance] > [Appliance Status]
- [Appliance] > [Appliance Interfaces]

[Appliance] > [Appliance Status]

次の表で [Administration] > [Settings] > [Appliance] > [Appliance Status] ページの各フィールドについて説明します。

表 7-1　[Appliance Status] の詳細

フィールド	説明
Configure Details	
Host Name	マシンのホスト名。ユーザ マシンのホスト名が DNS にない場合、IP アドレスが表示されます。
Domain Name	サーバのドメイン名。
Default Gateway	属しているネットワーク環境のデフォルト ゲートウェイの IP アドレスです。
DNS Server(s)	DNS サーバの IP アドレスです。各 DNS サーバは、この DHCP スコープで割り当てられた IP アドレスと一致するように、クライアントの DNS エントリを更新できる必要があります。
NTP Host(s)	NTP サーバの IP アドレスです。
Status Details	
Server Time	サーバのシステム時刻。
System Up Time	サーバが起動してからダウンタイムなしで稼働している時間の指標です。

表 7-1　[Appliance Status] の詳細 （続き）

フィールド	説明
Application Up Time	Prime Infrastructure が起動してからダウンタイムなしで稼働している時間の指標です。
Temperature Status	CPU 温度のステータス。
RAID Status	RAID(冗長ディスク アレイ）のステータス。
Fan Status	サーバの冷却ファンのステータス。
Power Supply Status	サーバの電源ユニットのステータス。
Inventory Details	
Memory	利用可能な総メモリ空間を表示します。
Disk Space	利用可能なディスク領域と使用済みのディスク領域、およびさまざまなアプライアンスによるディスク領域の使用率を表示します。
UDI Details	
Product Identifier	製品 ID は、デバイスのタイプを識別します。
Serial Number	シリアル番号は、デバイスを一意に識別する 11 桁の番号です。
Version Identifier	VID は製品のバージョンです。製品が改訂されるたびに、VID は増分されます。
Memory Utilization	当日のメモリ使用率を線グラフで表示します。
CPU Utilization	当日の CPU 使用率を線グラフで表示します。

[Appliance] > [Appliance Interfaces]

現在、[Administration] > [Settings] > [Appliance] > [Appliance Interfaces] ページは推奨されません。次回の Prime Infrastructure リリースで削除される予定です。

[Add User]

次に [Administration] > [Users, Roles & AAA] > [Users] ページの内容について説明します。[Add User] ページ：

- [Users, Roles & AAA] > [Users] > [Add User] > [Lobby Ambassador Defaults] タブ

[Users, Roles & AAA] > [Users] > [Add User] > [Lobby Ambassador Defaults] タブ

次の表で [Administration] > [Users, Roles & AAA] > [Users] > [Add Users] > [Lobby Ambassador Defaults] の各フィールドについて説明します。

表 7-2　[Users, Roles & AAA] > [Users] > [Add User] > [Lobby Ambassador Defaults]

フィールド	説明
Profile	ゲスト ユーザが接続するプロファイルを選択します。
User Role	ドロップダウン リストから、ゲスト ユーザのユーザ ロールを選択します。ユーザ ロールは、管理者により事前に定義され、ゲストのアクセス（契約者、顧客、代理店、ベンダー、ビジターなど）にアソシエートされています。 ユーザ ロールを使用して、ネットワーク内の特定のユーザに割り当てられた帯域幅の量を管理します。
Lifetime	ゲスト ユーザ アカウントをアクティブにしておく期間を次のオプションのいずれかを選択して定義します。 [Limited]：時間および分のドロップダウン リストを使用して、ゲスト ユーザ アカウントをアクティブにする期間を選択します。[Limited] のデフォルト値は、1 日（8 時間）です。 [Unlimited]：ゲスト アカウントの有効期限の日付はありません。
Apply to	ドロップダウン リストから、次のいずれかを選択します。 [Indoor Area]：キャンパス、ビルディング、フロア。 [Outdoor Area]：キャンパス、屋外領域。 [Controller List]：選択されたプロファイルが作成されたコントローラの一覧。 [Config Groups]：Prime Infrastructure で設定された設定グループ名。
Email Id	（オプション）ゲスト アカウント クレデンシャルの送信先のホストの電子メール ID を入力します。ロビー アンバサダー ユーザは、ゲスト ユーザの作成時に希望する電子メール ID を入力できます。
Description	このアカウントの説明を入力します。
Disclaimer	デフォルトの免責条項のテキストを入力します。
Defaults Editable	このチェックボックスをオンにすると、ロビー アンバサダーが設定済みのデフォルトのすべての値をオーバーライドできます。こうすることで、Lobby Ambassador が [Lobby Ambassador] ポータルからゲスト アカウントを作成する際にこれらのゲスト ユーザ アカウントのデフォルト設定を編集できるようになります。 デフォルトのプロファイルがこのタブで選択されていない場合、デフォルト値はロビー アンバサダーに適用されません。ただし、Lobby Ambassador アカウントは作成され、Lobby Ambassador は必要に応じてクレデンシャルを持ったユーザを作成できます。
Max User Creation Allowed	ロビー アンバサダーが指定する期間内に作成可能なゲスト ユーザ数を制限します。期間は、時間、日、または週で定義します。
Preview Current Logo	リンクをクリックして、現在使用されているロゴを参照します。さらにクリックして有効にするか、別の場所を参照してロゴを更新できます。
Print Page Header Text	追加のページ ヘッダーのテキスト情報を入力します。

[Guest Users]

次に、[Guest Users] > [Add Guest User] ページの各フィールドについて説明します。

- [Guest Users] > [Add Guest User] > [General] タブ
- [Guest Users] > [Add Guest User] > [Advanced] タブ

[Guest Users] > [Add Guest User] > [General] タブ

次の表で、[Services] > [Network Services] > [Guest Users] > [Add Guest User] > [General] の各フィールドについて説明します。

表 7-3　[Guest Users] > [Add Guest User] > [General] タブ フィールドの説明

フィールド	説明
User Name	ゲスト ユーザ名を入力します。最大長は 24 文字です。
Generate Password	ゲスト ユーザ アカウントの作成スケジュールごとにユーザ名とパスワードを生成するには、このチェックボックスをオンにします。これを有効化すると、異なるパスワードが毎日（選択した日数分）支給されます。これを無効化すると（オフにする）、1 つのパスワードが選択した日数の間支給されます。オプションとして、スケジュールごとに新しいパスワードを生成できます。
Password	パスワードを入力します。パスワードには、次のような要求事項があります。 • パスワードには少なくとも 8 文字必要です。 • 小文字、大文字、数字、特殊文字の 4 種類の文字から 3 種類以上を使用してパスワードを作成する必要があります。
Confirm Password	[Password] フィールドに入力したパスワードを再入力します。
Description	ゲスト ユーザ テンプレートの説明を入力します。
Disclaimer	デフォルトの免責条項のテキストを入力します。

[Guest Users] > [Add Guest User] > [Advanced] タブ

次の表で、[Guest User] > [Add Guest User] > [Advanced] の各フィールドについて説明します。

表 7-4　[Guest User] > [Add Guest User] > [Advanced] タブの説明

フィールド	説明
Import From File	ゲスト ユーザ テンプレートを一括してインポートするには、このチェックボックスをオンにします。
Profile	ゲスト ユーザが接続するプロファイルを選択します。

表 7-4　[Guest User] > [Add Guest User] > [Advanced] タブの説明（続き）

フィールド	説明
User Role	ドロップダウン リストから、ゲスト ユーザのユーザ ロールを選択します。ユーザ ロールは、管理者により事前に定義され、ゲストのアクセス（契約者、顧客、代理店、ベンダー、ビジターなど）にアソシエートされています。 ユーザ ロールを使用して、ネットワーク内の特定のユーザに割り当てられた帯域幅の量を管理します。
Lifetime	ゲスト ユーザ アカウントをアクティブにしておく期間を次のオプションのいずれかを選択して定義します。 [Limited]：時間および分のドロップダウン リストを使用して、ゲスト ユーザ アカウントをアクティブにする期間を選択します。[Limited] のデフォルト値は、1 日（8 時間）です。 [Unlimited]：ゲスト アカウントの有効期限の日付はありません。
Apply to	ドロップダウン リストから、次のいずれかを選択します。 [Indoor Area]：キャンパス、ビルディング、フロア。 [Outdoor Area]：キャンパス、屋外領域。 [Controller List]：選択されたプロファイルが作成されたコントローラの一覧。 [Config Groups]：Prime Infrastructure で設定された設定グループ名。