Cloud OnRamp for SaaS、Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r

簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます。**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ**への変更、および **Cisco コントローラ**から **Cisco Catalyst SD-WAN 制御コンポーネント**への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r を使用しているデバイスにのみ、この項で説明されているワークフローを使用します。以降のリリースについては、「Cloud OnRamp for SaaS, Cisco IOS XE Release 17.3.1a and Later」を参照してください。

この機能は、Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r で完全に機能するベータ版としてリリースされ、プロビジョニング ワークフローが将来のリリースで変更される可能性がありました。このワークフローは Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a で廃止され、Cisco IOS XE Catalyst SD-WAN デバイスおよび Cisco vEdge デバイスに対応する統合ワークフローに置き換えられました。

表 *1*: 機能の履歴

機能名	リリース情報	説明
Cloud OnRamp for SaaS、Cisco IOS XE Catalyst SD-WAN デバイス	Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r	Cloud OnRamp for SaaS は Cisco IOS XE Catalyst SD-WAN デバイスで使用できますが、設定ワークフローは Cisco vEdge デバイスに適用されるワークフローとはまったく異なります。 この機能は、Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r で完全に機能するベータ版としてリリースされています。プロビジョニング ワークフローは、将来のリリースで変更される可能性があります。

多くの組織は、ビジネスに不可欠な機能を Software-as-a-Service（SaaS）アプリケーションに依存しています。これらのクラウドベースのサービスには、Office365、Salesforce、Box などの、多くのサービスがあります。クラウドベースのサービスとして、これらの SaaS アプリケーションは、インターネット接続を介して使用可能な独自のリモートサーバーと通信する必要があります。

リモートサイトでは、SaaS アプリケーションによって次のような特別な課題が発生する可能性があります。

- **パフォーマンス**：ブランチオフィスなどのリモートサイトが、データセンターなどの一元化された場所を介して SaaS トラフィックをルーティングすると、パフォーマンスが低下し、遅延が発生してユーザー体験に影響を与えます。
- **ルーティングを最適化できない**：ネットワーク管理者が、これらの SaaS アプリケーションのパフォーマンスを可視化できない場合や、SaaS トラフィックのルーティングをより効率的なパスに変更できない場合があります。

Cloud OnRamp for SaaS（旧称 CloudExpress サービス）は、これらの課題に対処します。これにより、特定の SaaS アプリケーションおよびインターフェイスを選択し、SD-WAN が指定されたインターフェイスを使用して各 SaaS アプリケーションのパフォーマンスが最も高いパスを決定できるようになります。たとえば、以下を有効にすることができます。

- ブランチサイトでのダイレクト インターネット アクセス（DIA）接続を介したルーティング（使用可能な場合）
- 地域のデータセンターなどの、ゲートウェイの場所を介したルーティング

SD-WAN は各 SaaS アプリケーションの使用可能な各パスを継続的にモニターするため、1 つのパスで問題が発生した場合は、SaaS トラフィックを動的に調整して、より適切なパスに移動させることができます。

詳細については、『SD-WAN: Cloud OnRamp for SaaS Deployment Guide』を参照してください。

- 概要：Cloud onRamp for SaaS の設定方法 （3 ページ）
- Cloud onRamp for SaaS を使用する一般的なシナリオ （4 ページ）
- プローブ機能テンプレートの作成 （11 ページ）

• Cloud onRamp for SaaS のポリシーの作成 （14 ページ）

概要：Cloud onRamp for SaaS の設定方法

vEdge デバイスで Cloud onRamp for SaaS を使用するのとは異なり、Cisco XE SD-WAN デバイスの機能を設定するには、次の 2 つの手順を実行します。

- ベストパスの決定（機能テンプレートによって設定）
- ベストパスの使用（ポリシーによって設定）

次に、タスクの概要を示します。

	タスク	コンポーネント	まとめ
1	SaaS アプリケーションのベストパスの決定	機能テンプレート	特定の SaaS アプリケーションサーバーのパスをプローブするように Cloud onRamp for SaaS を設定する機能テンプレートを作成して、それぞれのベストパスを決定し、これらのパスに基づいてテーブルを作成します。 SD-WAN は定期的にプローブし、ベストパスに関する最新情報でテーブルを更新します。 トポロジにゲートウェイサイトとブランチサイトが含まれている場合は、ブランチサイトとゲートウェイサイトに個別の機能テンプレートが必要です。 「プローブ機能テンプレートの作成」を参照してください。 （注） プローブ機能テンプレートは、Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r 以降のリリースではサポートされていません。

	タスク	コンポーネント	まとめ
2	SaaS アプリケーションのベストパスの使用	ポリシー	前の手順で決定されたベストパスを使用するように特定の SaaS アプリケーションに指示するポリシーを作成します。 （注） このポリシーでは、機能テンプレートに含まれている SaaS アプリケーションのみを指定します。機能テンプレートに含まれていない SaaS アプリケーションがこのポリシーで指定されている場合、そのアプリケーションのトラフィックは、Cloud onRamp for SaaS が有効になっていない場合と同様にデフォルトのパスを使用します。 「Cloud onRamp for SaaS のポリシーの作成」を参照してください。

Cloud onRamp for SaaS を使用する一般的なシナリオ

SD-WAN を使用している組織の場合、通常、ブランチサイトはデフォルトで SaaS アプリケーション トラフィックを SD-WAN オーバーレイリンク経由でデータセンターにルーティングします。データセンターから、SaaS トラフィックは SaaS サーバーに到達します。

たとえば、中央データセンターとブランチサイトがある大規模な組織で、従業員がブランチサイトで Office 365 を使用する場合があります。デフォルトでは、ブランチサイトの Office 365 トラフィックは、SD-WAN オーバーレイリンクを介して中央データセンターにルーティングされ、そこから Office 365 クラウドサーバーにルーティングされます。

シナリオ 1：ブランチサイトにダイレクト インターネット アクセス（DIA）接続がある場合は、データセンターをバイパスしてその直接ルートを介して SaaS トラフィックをルーティングすることで、パフォーマンスを向上させることができます。

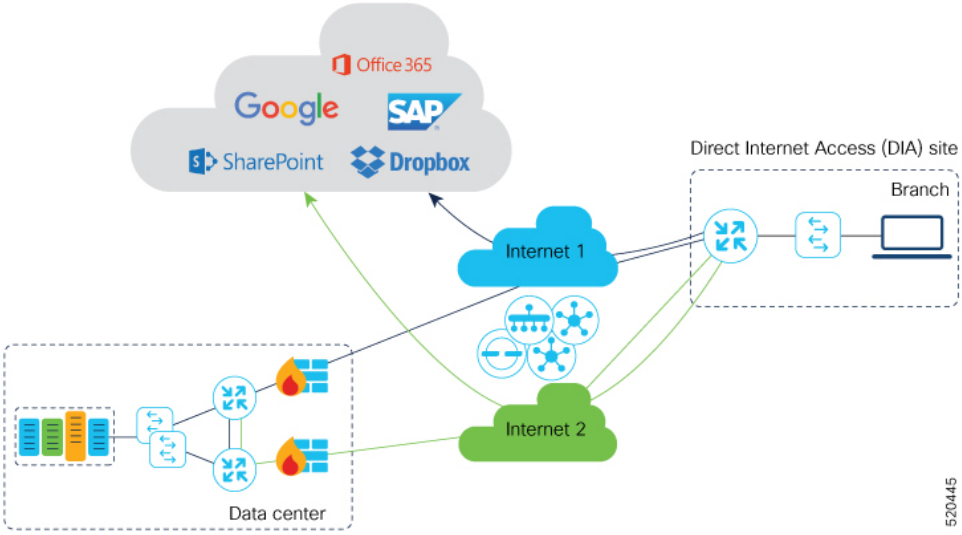
シナリオ 2：DIA リンクがあるゲートウェイサイトにブランチサイトが接続する場合、SaaS トラフィックがゲートウェイサイトの DIA を使用できるようにすることができます。

シナリオ 3：ハイブリッド方式。

シナリオ1：ダイレクトインターネットアクセスリンクを介したクラウドアクセス

このシナリオでは、次の図に示すように、ブランチサイトに 1 つ以上のダイレクト インターネット アクセス（DIA）リンクがあります。

Cloud onRamp for SaaS を使用すると、SD-WAN は、DIA リンクまたは SD-WAN オーバーレイリンクを介して、各 SaaS アプリケーションに最適な接続を選択できます。最適な接続は、SaaS アプリケーションによって異なる場合があることに注意してください。たとえば、Office365 のトラフィックはある 1 つのリンクを介すると高速になり、Dropbox のトラフィックは別のリンクを介すると高速になる可能性があります。



設定ワークフロー

ブランチサイト専用のプローブ機能テンプレートを作成し、Cloud onRamp for SaaS を使用するためのポリシーを設定します。

	タスク	詳細
ブランチ サイト		

	タスク	詳細

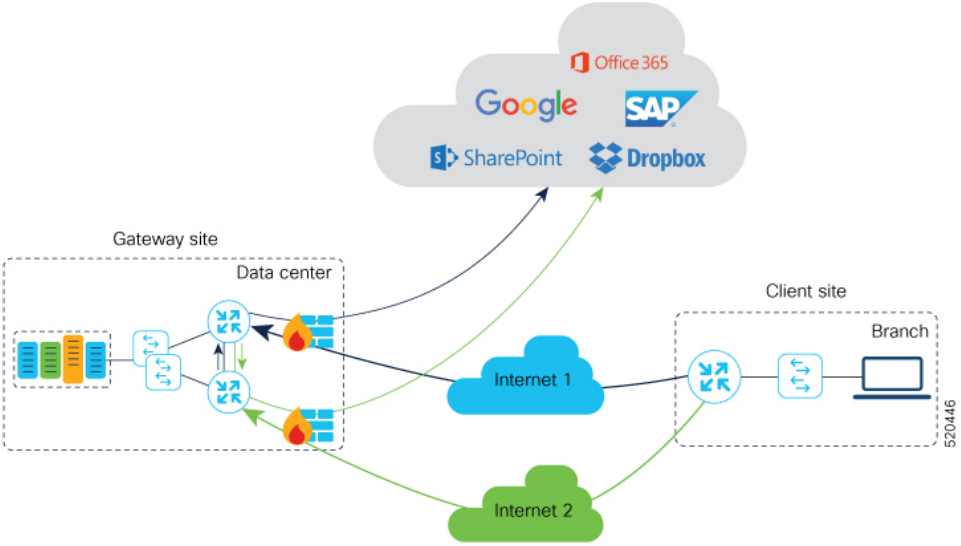
1	ブランチサイトのプローブ機能テンプレートを作成します。	プローブ機能テンプレートで、次のようにパラメータを設定します。
		• [SaaS Mode]：[SaaS Branch]
		• [TLOCS]：[All DIA TLOC] または [TLOC List] を選択して、ドロップダウンメニューでTLOCの色を選択します。
		  • [All DIA TLOC]：ブランチのすべての TLOC に対して DIA が有効になっている場合は、このオプションを選択します。
		  • [TLOC List]：サイトの一部の TLOC でのみ DIA が有効になっている場合は、このオプションを選択してから、DIA が有効になっている TLOC に対応する色を選択できます。
		• [SaaS applications]：Cloud onRamp for SaaS のアプリケーションを指定します。
		「プローブ機能テンプレートの作成」を参照してください。

2	ブランチサイトのデバイステンプレートで機能テンプレートを使用します。	デバイステンプレートの [Additional Templates] セクションの [Probes] フィールドで、前の手順で作成した機能テンプレートを選択します。
3	デバイステンプレートをブランチサイトに適用します。	
ポリシー		
4	ポリシーを作成します。	アプリケーションルートポリシーの一致条件で、クラウドSaaSアプリケーションを選択し、機能テンプレートの作成時に指定したものと同じアプリケーションを指定します。アクションとして [Cloud SLA] を選択します。 「Cloud onRamp for SaaS のポリシーの作成」を参照してください。
5	ポリシーをアクティブにします	以前に作成した機能テンプレートが適用されたブランチサイトにポリシーを適用します。

シナリオ 2：ゲートウェイサイトを介したクラウドアクセス

このシナリオでは、ブランチサイトにゲートウェイサイトへの直接接続が 1 つ以上あり、ゲートウェイサイトにインターネットへのリンクがあります。

Cloud onRamp for SaaS を使用すると、SD-WAN は、ゲートウェイサイトを介して、各 SaaS アプリケーションに最適な接続を選択できます。ブランチサイトが複数のゲートウェイサイトに接続している場合、異なるゲートウェイサイトを通過する場合でも、SD-WAN は各 SaaS アプリケーションについて SaaS トラフィックがベストパスを使用するようにします。



設定ワークフロー

ブランチサイトとゲートウェイサイトのプローブ機能テンプレートを作成し、Cloud onRamp for SaaS を使用するためのポリシーを設定します。

	タスク	詳細
ブランチ サイト		

	タスク	詳細
1	ブランチサイトのプローブ機能テンプレートを作成します。	プローブ機能テンプレートで、次のようにパラメータを設定します。 • [SaaS Mode]：[SaaS Branch] • [TLOCS]：[All DIA TLOC] • [SaaS applications]：アプリケーションを指定しません。 （注） シナリオ 1（ダイレクト インターネット アクセス リンクを介したクラウドアクセス）と比較して、このワークフローの違いに注意してください。このワークフローでは、ゲートウェイサイト設定でアプリケーションを指定します（以下を参照）。 「プローブ機能テンプレートの作成」を参照してください。
2	ブランチサイトのデバイステンプレートで機能テンプレートを使用します。	デバイステンプレートの [Additional Templates] セクションの [Probes] フィールドで、前の手順で作成した機能テンプレートを選択します。
3	デバイステンプレートをブランチサイトに適用します。	
ゲートウェイサイト		
4	ゲートウェイサイトのプローブ機能テンプレートを作成します。	• ゲートウェイサイトが同一のルータとインターフェイスを使用していない限り、各ゲートウェイサイトには個別の機能テンプレートが必要です。 • [SaaS Mode]：[SaaS Gateway] [SaaS Gateway] を選択した後に、プローブを開始するインターフェイス名を指定します。このインターフェイスは、ゼロ以外の VPN にバインドする必要があります。 • [SaaS applications]：Cloud onRamp for SaaS のアプリケーションを指定します。 「プローブ機能テンプレートの作成」を参照してください。

	タスク	詳細
5	ゲートウェイサイトのデバイステンプレートで、前の手順で作成した機能テンプレートを使用します。	デバイステンプレートの [Additional Templates] セクションの [Probes] フィールドで、前の手順で作成した機能テンプレートを選択します。
6	デバイステンプレートをゲートウェイサイトに適用します。	
ポリシー		
7	ポリシーを作成します。	上記のタスク 4 の機能テンプレートと同じアプリケーションを指定します。 「Cloud onRamp for SaaS のポリシーの作成」を参照してください。
8	ポリシーをアクティブにします。	以前に作成した機能テンプレートが適用されたブランチサイトおよびゲートウェイサイトにポリシーを適用します。

シナリオ 3：ハイブリッドアプローチ

このシナリオでは、ブランチサイトには、ダイレクトインターネットアクセス（DIA）リンクと、インターネットへのリンクもあるゲートウェイサイトへのリンクの両方があります。

Cloud onRamp for SaaS を使用すると、SD-WAN は、DIA リンクまたはゲートウェイサイトを介して、各 SaaS アプリケーションに最適な接続を選択できます。

設定ワークフロー

ブランチサイトとゲートウェイサイトのプローブ機能テンプレートを作成し、Cloud onRamp for SaaS を使用するためのポリシーを設定します。

	タスク	詳細
ブランチ サイト		

	タスク	詳細

1	ブランチサイトのプローブ機能テンプレートを作成します。	プローブ機能テンプレートで、次のようにパラメータを設定します。
		• [SaaS Mode]：[SaaS Branch]
		• [TLOCS]：[All DIA TLOC] または [TLOC List] を選択して、ドロップダウンメニューでTLOCの色を選択します。
		  • [All DIA TLOC]：ブランチのすべての TLOC に対して DIA が有効になっている場合は、このオプションを選択できます。
		  • [TLOC List]：サイトの一部の TLOC でのみ DIA が有効になっている場合は、このオプションを選択してから、DIA が有効になっている TLOC に対応する色を選択できます。
		• [SaaS applications]：アプリケーションを指定します。
		「プローブ機能テンプレートの作成」を参照してください。

2	ブランチサイトのデバイステンプレートで機能テンプレートを使用します。	デバイステンプレートの [Additional Templates] セクションの [Probes] フィールドで、前の手順で作成した機能テンプレートを選択します。
3	デバイステンプレートをブランチサイトに適用します。	
ゲートウェイサイト		

	タスク	詳細
4	ゲートウェイサイトのプローブ機能テンプレートを作成します。	• ゲートウェイサイトが同一のルータおよびインターフェイスを使用していない限り、各ゲートウェイサイトには個別の機能テンプレートが必要です。 • [SaaS Mode]：[SaaS Gateway] [SaaS Gateway] を選択した後に、プローブを開始するインターフェイス名を指定します。このインターフェイスは、ゼロ以外の VPN にバインドする必要があります。 • [SaaS applications]：Cloud onRamp for SaaS のアプリケーションを指定します。 「プローブ機能テンプレートの作成」を参照してください。
5	ゲートウェイサイトのデバイステンプレートで、前の手順で作成した機能テンプレートを使用します。	デバイステンプレートの [Additional Templates] セクションの [Probes] フィールドで、前の手順で作成した機能テンプレートを選択します。
6	デバイステンプレートをゲートウェイサイトに適用します。	
ポリシー		
7	ポリシーを作成します。	上記のタスク 4 の機能テンプレートと同じアプリケーションを指定します。 「Cloud onRamp for SaaS のポリシーの作成」を参照してください。
8	ポリシーをアクティブにします。	以前に作成した機能テンプレートが適用されたブランチサイトおよびゲートウェイサイトにポリシーを適用します。

プローブ機能テンプレートの作成

（注） プローブ機能テンプレートは、Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r 以降のリリースではサポートされていません。

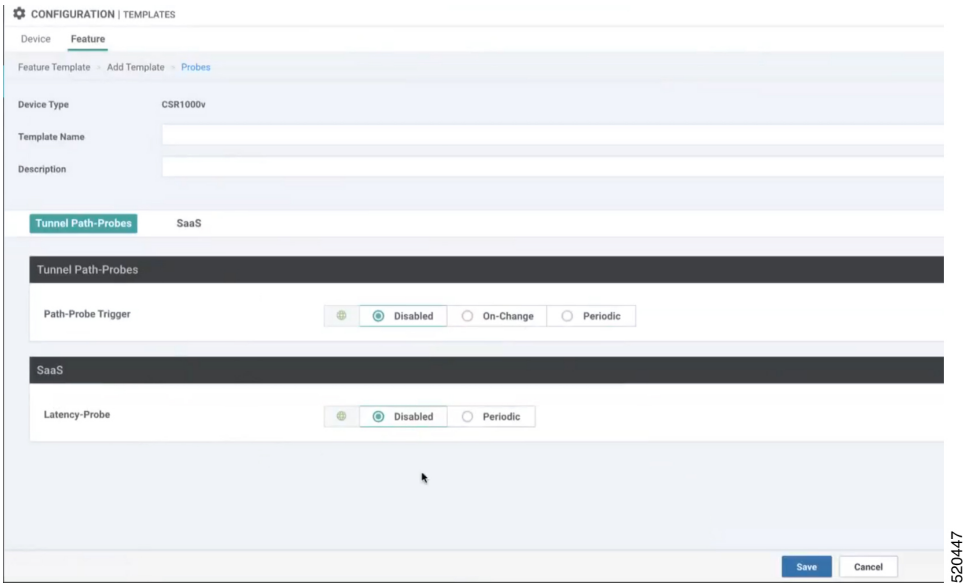
Cisco XE SD-WAN デバイスで Cloud OnRamp for SaaS を使用するためのプローブテンプレートを作成するには、次の手順を実行します。

ブランチサイトまたはゲートウェイサイトに適用する機能テンプレートを作成します。テンプレートの [SaaS Mode] オプションで、ブランチサイトとゲートウェイサイトのどちらでテンプレートを使用するかを決定します。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Templates]** の順に選択します。
2. [Feature Templates] をクリックします。

（注） Cisco vManage リリース 20.7.1 以前のリリースでは、[Feature Templates] のタイトルは [Feature] です。

3. [Add template] をクリックします。
4. デバイスモデルを選択します。
5. [Other Templates] で [Probes] をクリックして、Cloud OnRamp for SaaS のプローブテンプレートを作成します。



6. 必要に応じて、次のフィールドを設定します。一部のオプションを選択すると、他のフィールドで使用できるオプションが変更されます。

フィールド	説明
Tunnel Path-Probes	
Path-Probe Trigger	[Disabled] に設定する必要があります。 （注） 本リリースではサポートされていません。

フィールド	説明
Latency-Probe	[Disabled]：この機能テンプレートで Cloud OnRamp for SaaS が無効になります。 [Periodic]：Cloud OnRamp for SaaS が有効になります。
Latency-Probe Frequency	サイトと SaaS アプリケーション クラウド サーバー間のリンクをプローブする頻度（秒）。プローブは、利用可能な各パスの遅延を判断します。 範囲：0 ～ 65535 デフォルト：30 （注） 推奨：デフォルト値の 30
SaaS Mode	この機能テンプレートのサイトのタイプを選択します。 [SaaS Branch]：ブランチサイトに適用される機能テンプレートの場合。 [SaaS Gateway]：ゲートウェイサイトに適用される機能テンプレートの場合。
TLOCS	（[SaaS Mode] の [SaaS Branch] オプションで利用可能） [All DIA TLOC]：有効な色が割り当てられている、サイトのすべてのダイレクト インターネット アクセス（DIA）インターフェイスを含めます。 [TLOC List]：1 つ以上の色を指定して、含めるインターフェイスを示します。これらのインターフェイスは、SaaS トラフィックで見込まれるルーティングパスを判断します。
TLOCS List Color	（[TLOCS] の [TLOC List] オプションで利用可能） ドロップダウンリストを使用して色を選択します。複数の色を選択できます。
Interface [x]	（[SaaS Mode] の [SaaS Gateway] オプションで利用可能） ゲートウェイサイトの 1 つ以上のインターフェイス名を指定します。機能テンプレートは、これらのインターフェイスのみに適用されます。 例：gig2/0
Path-Probe	[Disabled] に設定する必要があります。 （注） 本リリースではサポートされていません。

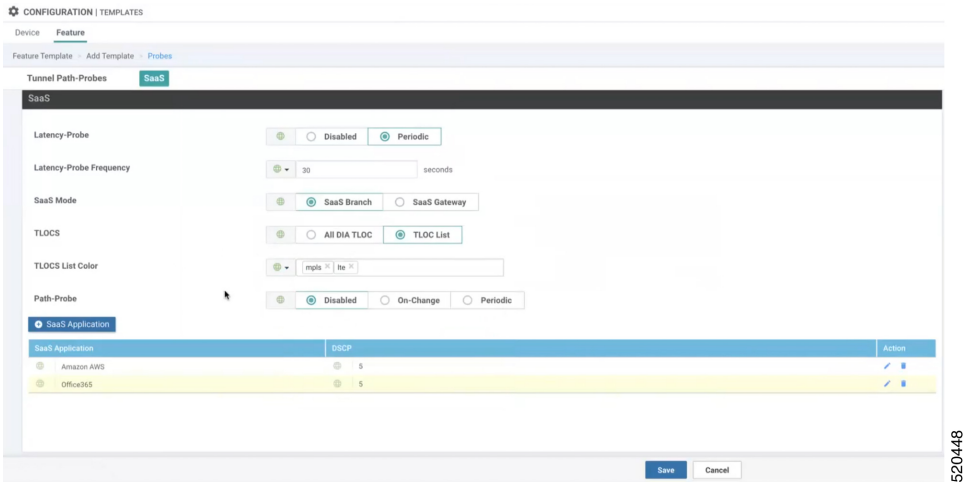
7. [SaaS Application] をクリックして、次のフィールドを表示します。これらのフィールドを使用して、SaaS アプリケーションを指定します。このプロセスを繰り返して、さらにアプリケーションを追加します。

アプリケーションを指定すると、このウィンドウの SaaS アプリケーションテーブルに表示されます。このテーブルには、リスト内のアプリケーションを編集または削除するオプションを備えたアクション列が含まれています。

フィールド	説明
SaaS App	ドロップダウンメニューを使用してアプリケーションを選択します。
DSCP	（注） Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a 以降では、Cisco SD-WAN Manager CoR SaaS ワークフローはこのオプションをプッシュしません。指定された DSCP 値は、この設定オプションを有効にした場合でも使用されません。 Differentiated Services Code Point（DSCP）の整数値を入力します。値を入力する必要がありますが、システムでは使用されません。異なるアプリケーションに同じ DSCP 値を割り当てることができます。 範囲：0 ～ 63

8. [保存（Save）] をクリックして、テンプレートを保存します。

   例：以下の例は、mpls および lte インターフェイスを含むブランチサイト用に設定されたプローブ機能テンプレートを示しています。これにより、Amazon AWS および Office365 SaaS アプリケーションのベストパスを決定します。



9. デバイステンプレートで機能テンプレートを使用するには、次の手順を実行します。

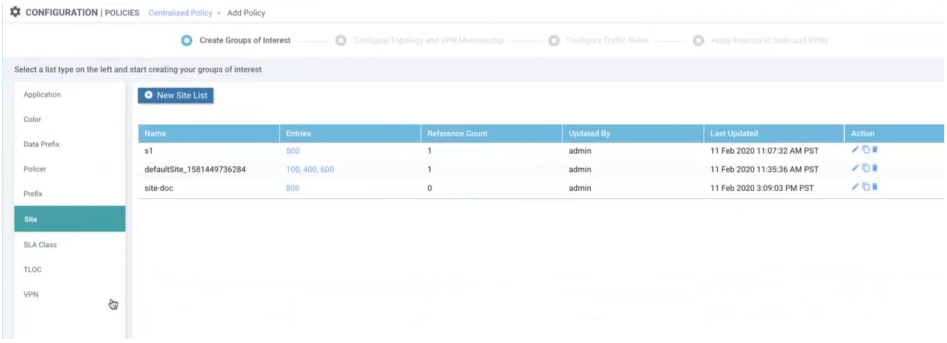
   デバイステンプレートの [Additional Templates] の [Probes] フィールドで、前述の手順で作成した機能テンプレートを選択します。

Cloud onRamp for SaaS のポリシーの作成

1. [Configuration] > [Policy] を選択します。

2. [Centralized Policy] タブをクリックします。
3. [Add Policy] をクリックします。
4. 左側のペインで、[Site] をクリックします。
5. ポリシーを適用するサイトのリストを作成します。このリストは後の手順で使用します。
   1. [新しいサイトリスト（New Site List）] をクリックします。
   2. [Site List Name] フィールドに、サイトリスト名を入力します。
   3. [Add Site] フィールドに、1 つ以上のサイト番号を入力します。
   4. [Add] をクリックします。

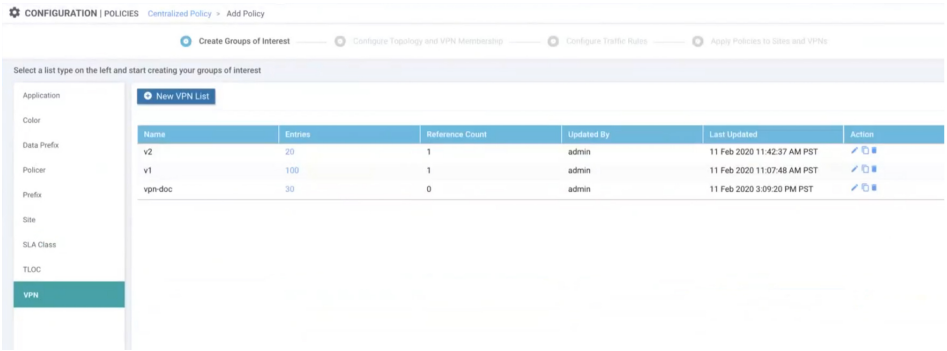
      サイトがサイトのテーブルに追加されます。



520449

6. 左側のペインで、[VPN] を選択します。
7. ポリシーを適用する VPN のリストを作成します。このリストは後の手順で使用します。
   1. [新しいVPNリスト（New VPN List）] をクリックします。
   2. [VPN List Name] フィールドに、VPN リストの名前を入力します。
   3. [Add VPN] フィールドに、1 つ以上の番号を入力します。
   4. [Add] をクリックします。

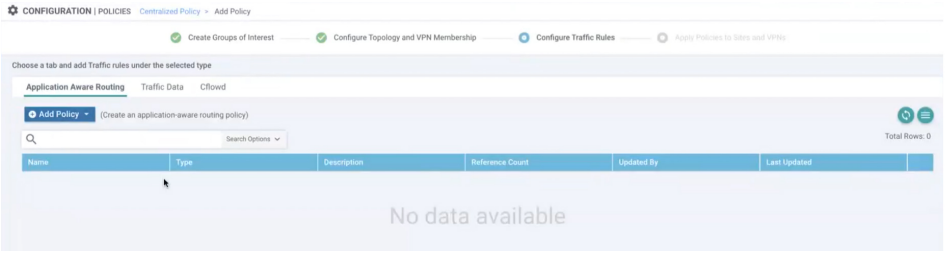
      VPN が VPN のテーブルに追加されます。



520450

8. [Next] を 2 回クリックして、[Configure Traffic Rules] ステップを表示します。

   [Application Aware Routing] タブがデフォルトで選択されています。

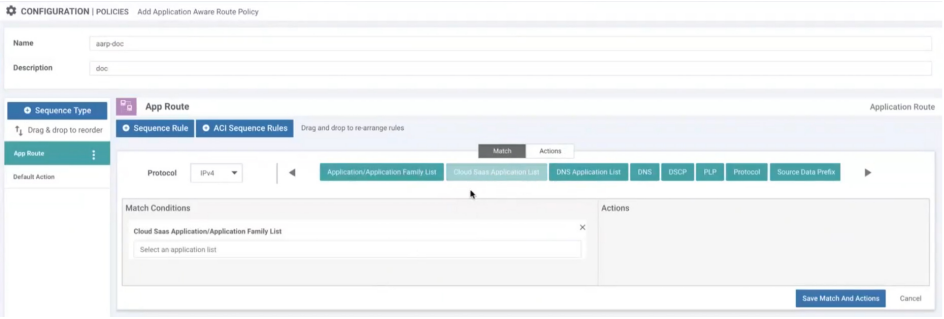


520451

9. [Add Policy] をクリックし、[Create New] を選択します。

10. ポリシーを作成します。

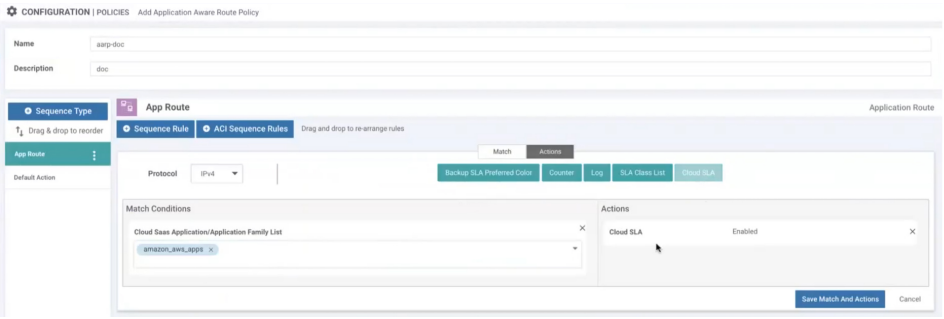
    1. ポリシーの名前と説明を入力します。
    2. [シーケンスタイプ（Sequence Type）] をクリックします。
    3. [Sequence Rule] をクリックします。
    4. デフォルトの [Match] が選択されている状態で、[Cloud SaaS Application List] をクリックします。



520452

    5. [Match Conditions] セクションで、SaaS アプリケーションを指定します。この SaaS アプリケーションで、Cloud onRamp for SaaS が有効になります。
    6. [アクション（Actions）] をクリックします。
    7. [クラウドSLA（Cloud SLA）] をクリックします。

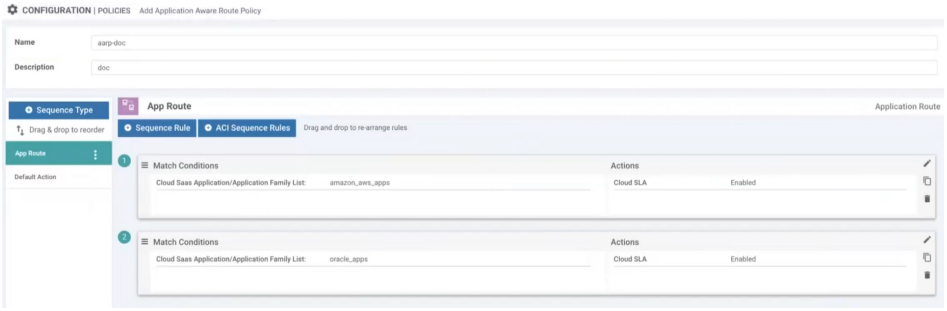
       [Actions] セクションに、[Cloud SLA Enabled] と表示されます。



520453

8. [一致とアクションの保存（Save Match and Actions）] をクリックします。
9. このポリシーに別の SaaS アプリケーションを追加するには、[Sequence Rule] を再度クリックし、10c の手順に従います。

   次の例は、一致条件とアクションを含む2つのシーケンスルールを示しています。各ルールは単一の SaaS アプリケーションを指定しています。



520454

10. [アプリケーション認識型ルーティングポリシーの保存（Save Application Aware Routing Policy）] をクリックします。
11. [Next] をクリックして、[Apply Policies to Sites and VPNs] ステップを表示します。
12. [Application-Aware Routing] タブをクリックします。
13. ポリシーを選択します。
14. [New Site List and VPN List] をクリックします。この手順で前に作成したサイトリストと VPN リストを選択します。
15. [Add] をクリックします。
16. [Save Policy] をクリックします。

11. ポリシーをアクティブにします。
    1. [Configuration] > [Policies] を選択します。
    2. ポリシーのリストで、アクティブ化するポリシーを見つけます。[more actions]（...）ボタンをクリックし、[Activate] を選択して、サイト ID によってポリシーで指定されたデバイスにポリシーをプッシュします。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。