2021年6月30日リリース
Mist 新機能のご紹介

ジュニパーネットワークス株式会社

JUNIPer
driven by Mist AI™

はじめに

- 本ドキュメントは2021年7月時点のMist cloudのGUIを使用しております
- 実際の画面と表示が異なる場合がございます
- 内容について不明な点、ご質問等がございましたら担当営業までお問い合わせください

本リリースで追加された機能一覧

Marvis

- “Other Action”の追加
- 継続的に接続に失敗するクライアントの表示
- ポートフラップの検知
- 会話型インターフェースの新しく改善されたクエリ

Simplified Operations

- ヘルプメニュー「クラウドステータス」と「ポートとエンドポイント」の追加
- クラウドステータス
- ポートとエンドポイント
- OrganizationのWebhook　監査ログとデバイスステータスログのサポート
- ネットワークセキュリティ–BSSIDワイルドカード
- マップのインポート–デバイスプロファイル

Wired Assurance

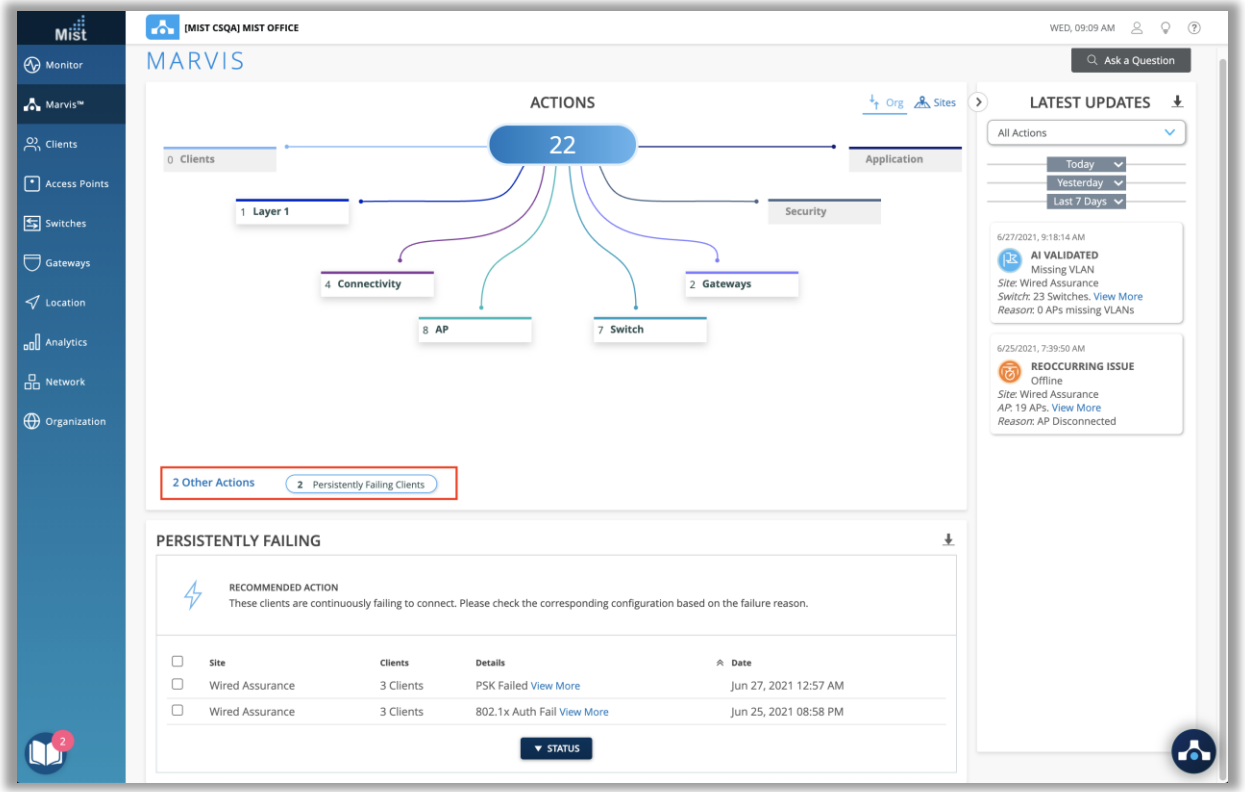
- バーチャルシャーシ
- OSPF　エリアとルーティングの設定[ベータ]

Mist Edge

- スプリットトンネリング

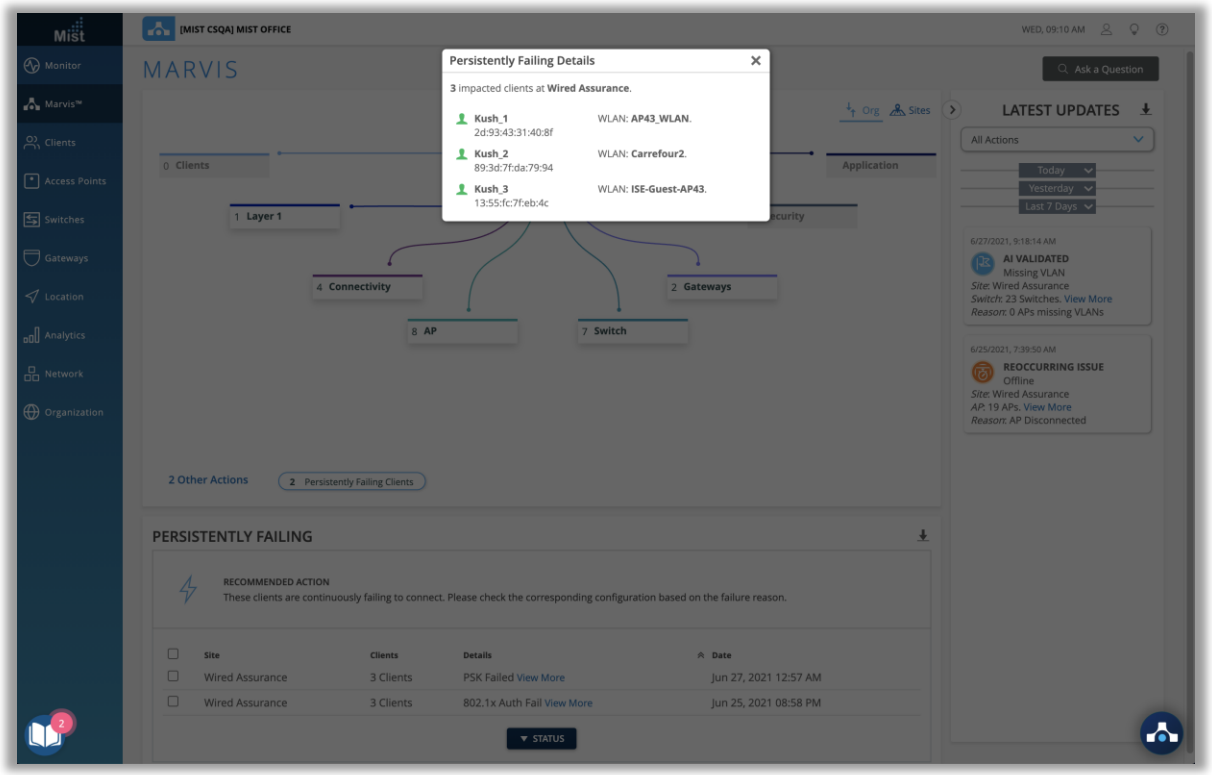
Marvis

Marvis
“Other Action”の追加



- “Other Action”は、Marvisアクションダッシュボードの新しいセクションです
- このセクションの目的は、緊急性が低く、即時のアクションを必要としない、Org全体の他のアクションを検知することです
- [**Other Action**]をクリックして、メインのアクションダッシュボード図の下にあるこの新しいセクションを見つけます
- これにより、**継続的に接続に失敗するクライアント**をリスト表示できます

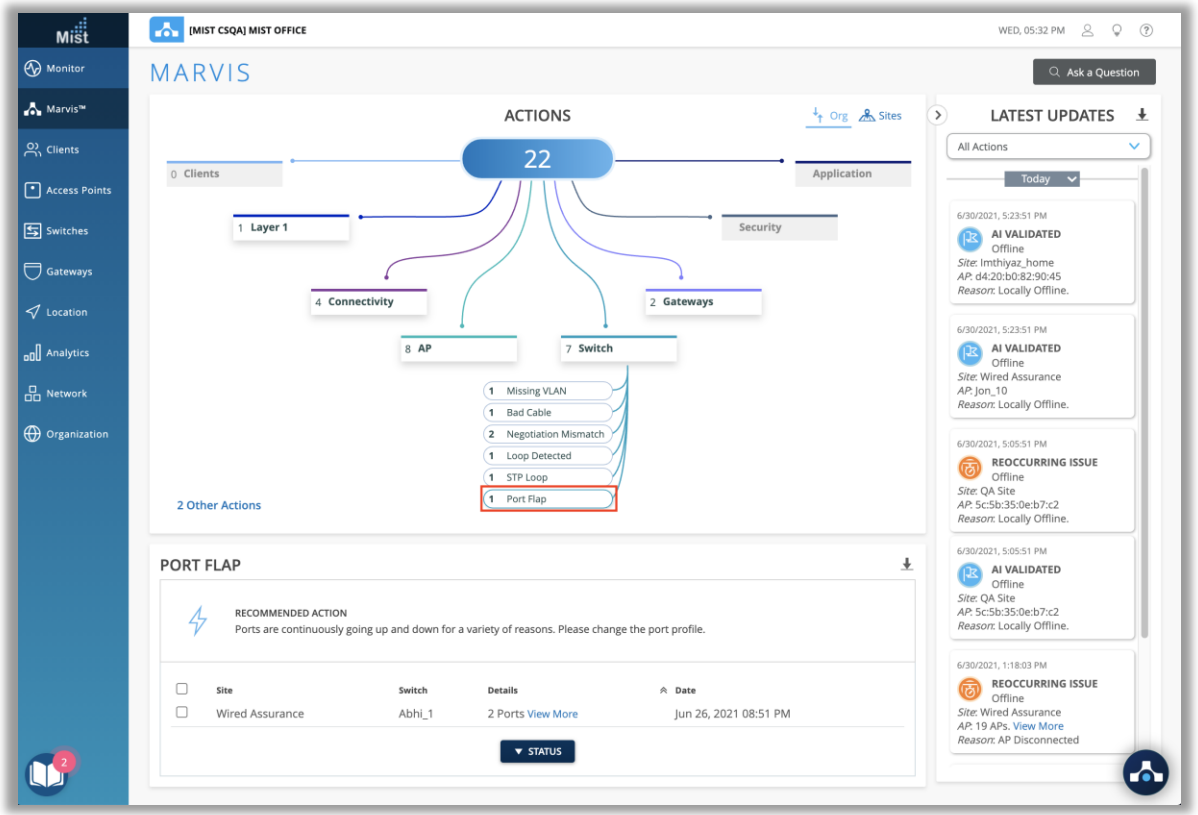
Marvis
継続的に接続に失敗するクライアントの表示



- [**Other Action**]セクションで利用できる最初のアクションは、クライアント固有の問題が原因で接続に継続的に失敗しているクライアントの表示です
  - 失敗の範囲はAP、WLAN、またはサーバーではありません
  - 間違ったPSKの入力による認証の失敗、または誤った802.1x構成が原因の失敗が原因である可能性があります

- [**View more**]リンクをクリックして、障害が発生しているクライアントのリストと、接続しようとしているWLANを確認します

Marvis Action
ポートフラップの検知

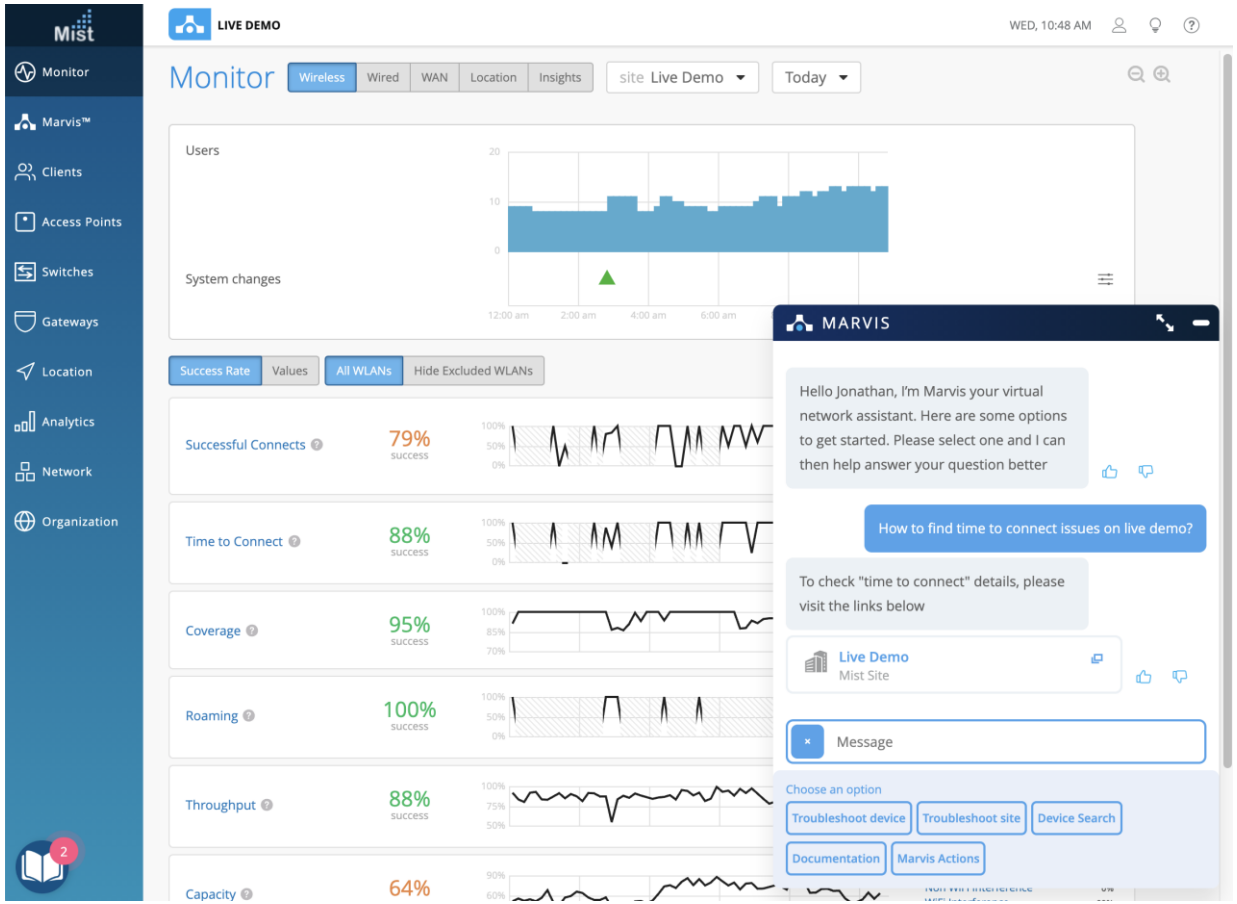


- ポートフラップは、アクションダッシュボードの**[Switch]**セクションで使用できる新しいアクションです
- このアクションにより、さまざまな理由で継続的にアップおよびダウンしているスイッチのポートが識別されます
- ポートのフラッピングは、接続の信頼性の低さ、ポートに接続されているデバイスの継続的な再起動、不適切なデュプレックス構成などが原因である可能性があります

会話型インターフェースの新しく改善されたクエリ

本リリースでは、いくつかの一般的なクエリを改善し、製品検索の新しいサポートを追加しました

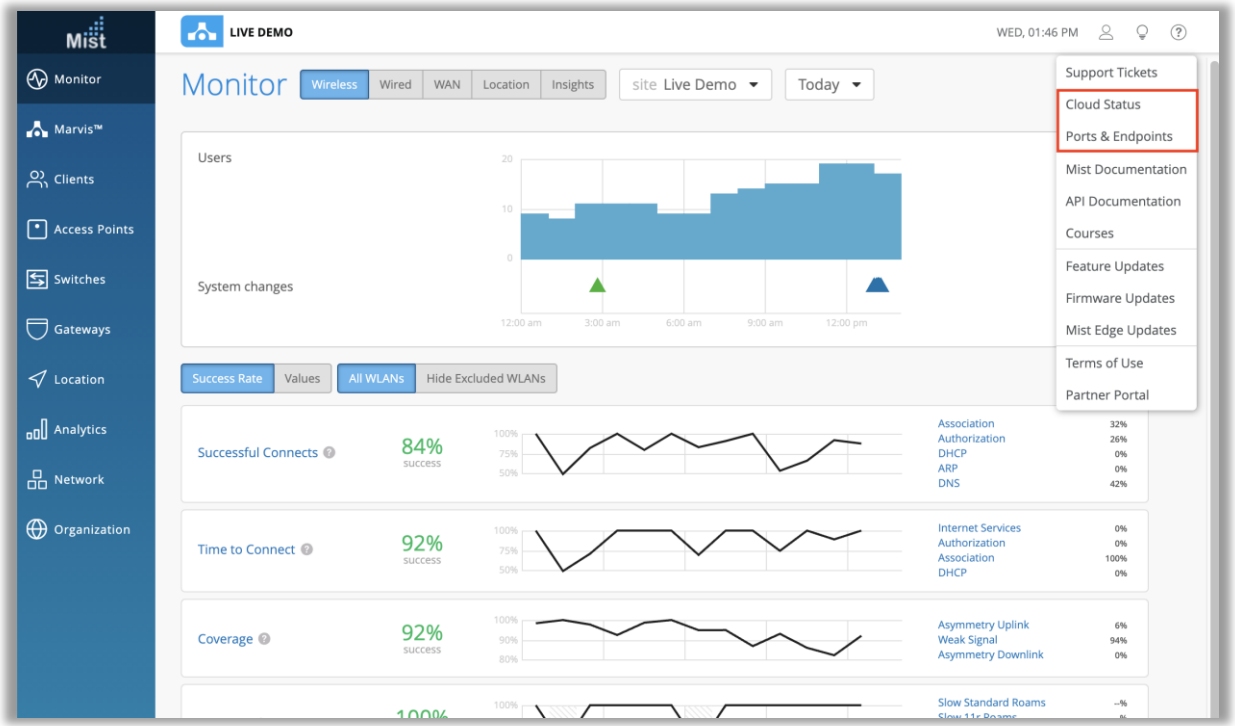
- 会話型インターフェースで次のタイプの問題を検索できるようになりました
  - Time to Connect
  - Successful Connects
  - Coverage
  - Roaming
  - Throughput
  - Capacity
  - Ap Uptime
  - Switch health
  - Association
  - Authorization
  - DHCP issues
  - DNS issue
  - ARP
  - Asymmetry Uplink
  - Asymmetry Downlink
  - OKC
  - Authentication



例：**“How to find time to connect issues at <name>”**では、Time to Connect SLEのUIに移動します

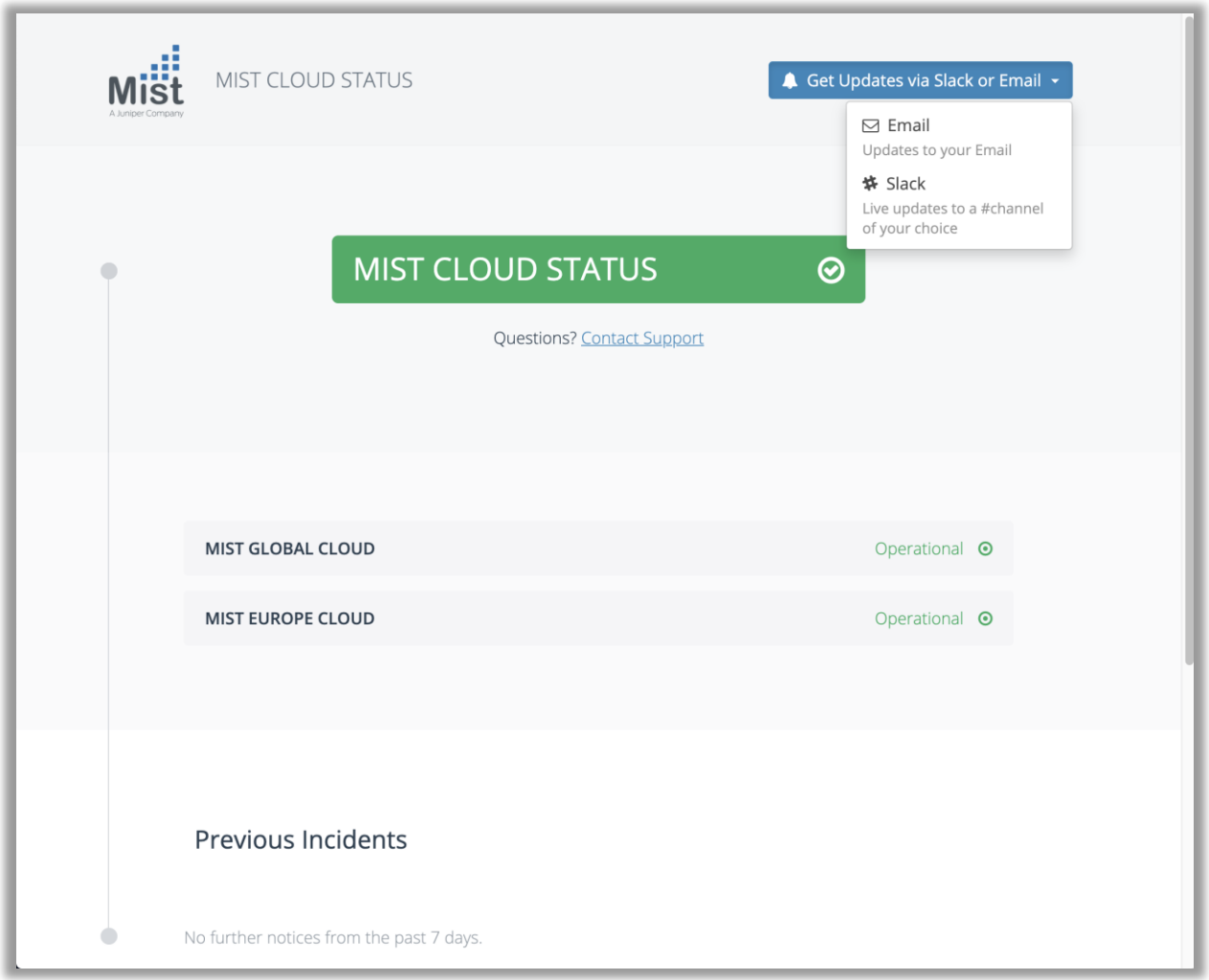
Simplified Operations

ヘルプメニュー
「クラウドステータス」と「ポートとエンドポイント」の追加



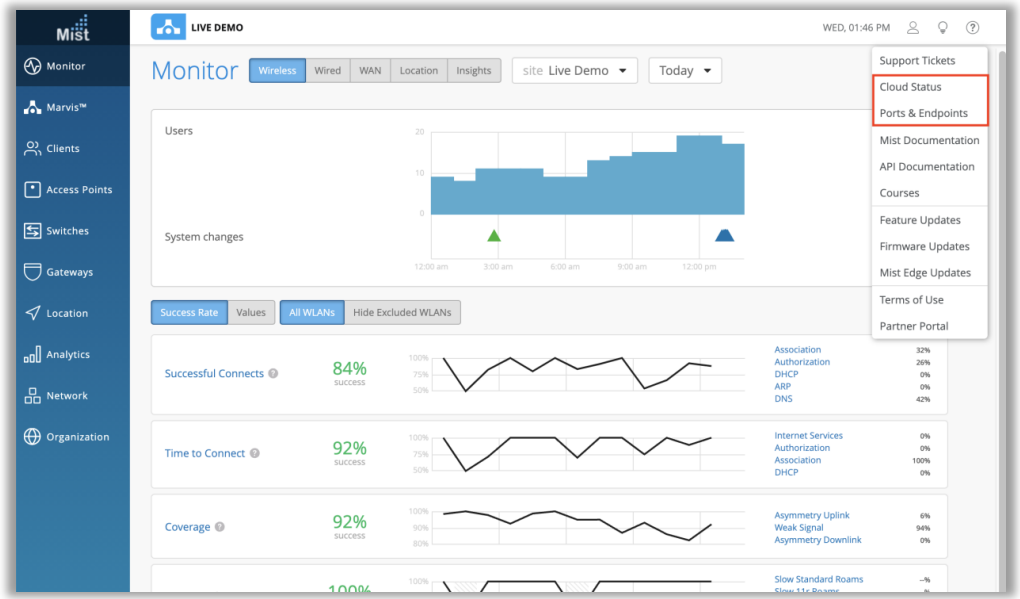
- ミストダッシュボードのどのページからでもアクセスできる2つの新しいアイテムをヘルプメニューに追加しました
- このメニューは、**？ボタン**で表示される右上隅にあります

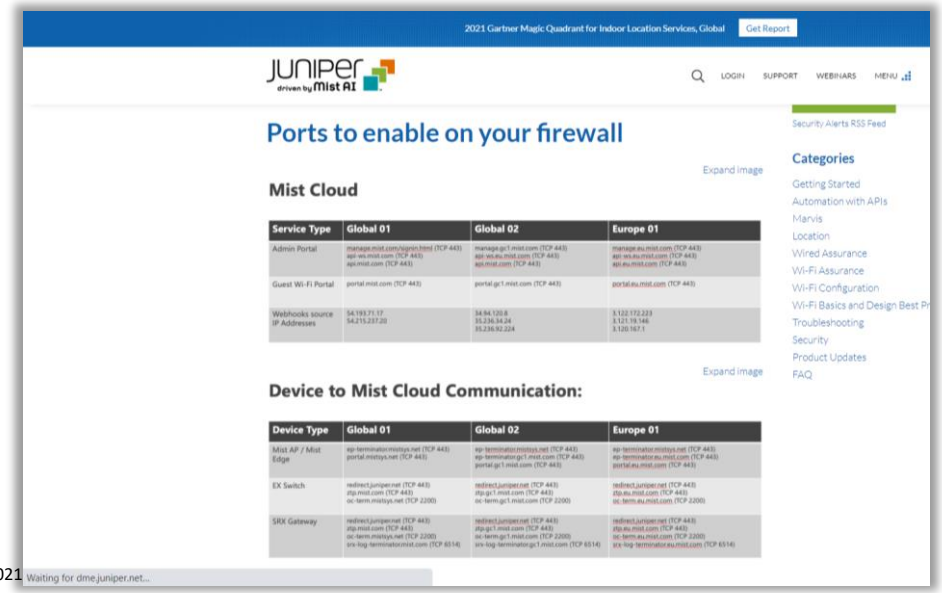
クラウドステータス



- クラウドステータスページ（https://status.mist.com/）にアクセスして、グローバルクラウドとEUクラウドの両方のミストクラウドステータスを監視します
- ここでは、クラウドが動作しているかどうか、またはエラーが発生しているかどうかを確認できます
- 過去7日間の過去のインシデントも一覧表示されます
- このページに手動で移動して確認せずにクラウドステータスの変更を通知したい場合は、ドロップダウンメニューでEメールまたはSlack通知にサインアップすることもできます

ポートとエンドポイント



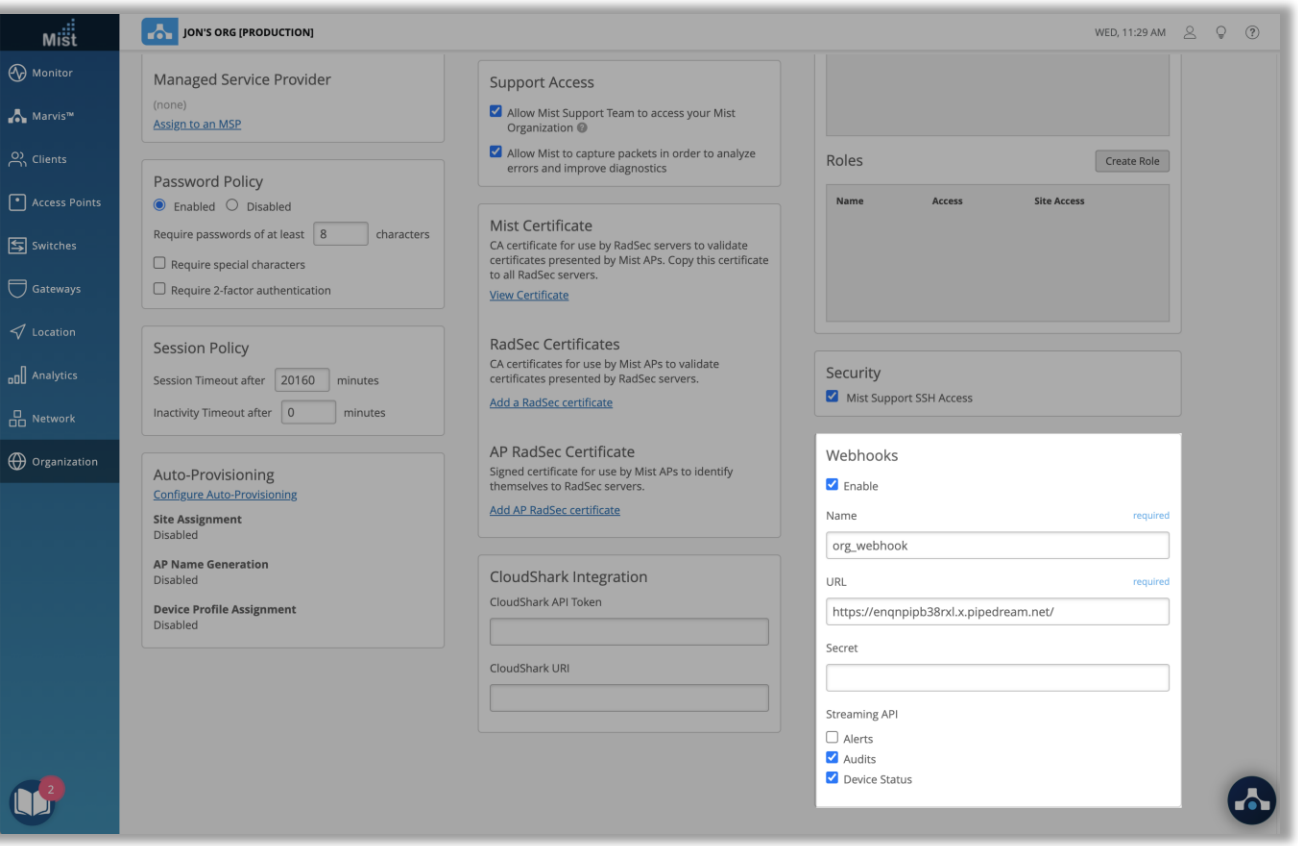


- Ports＆Endpointsをクリックすると、ドキュメントポータルの以下のページに移動します

  https://www.mist.com/documentation/ports-enable-firewall/

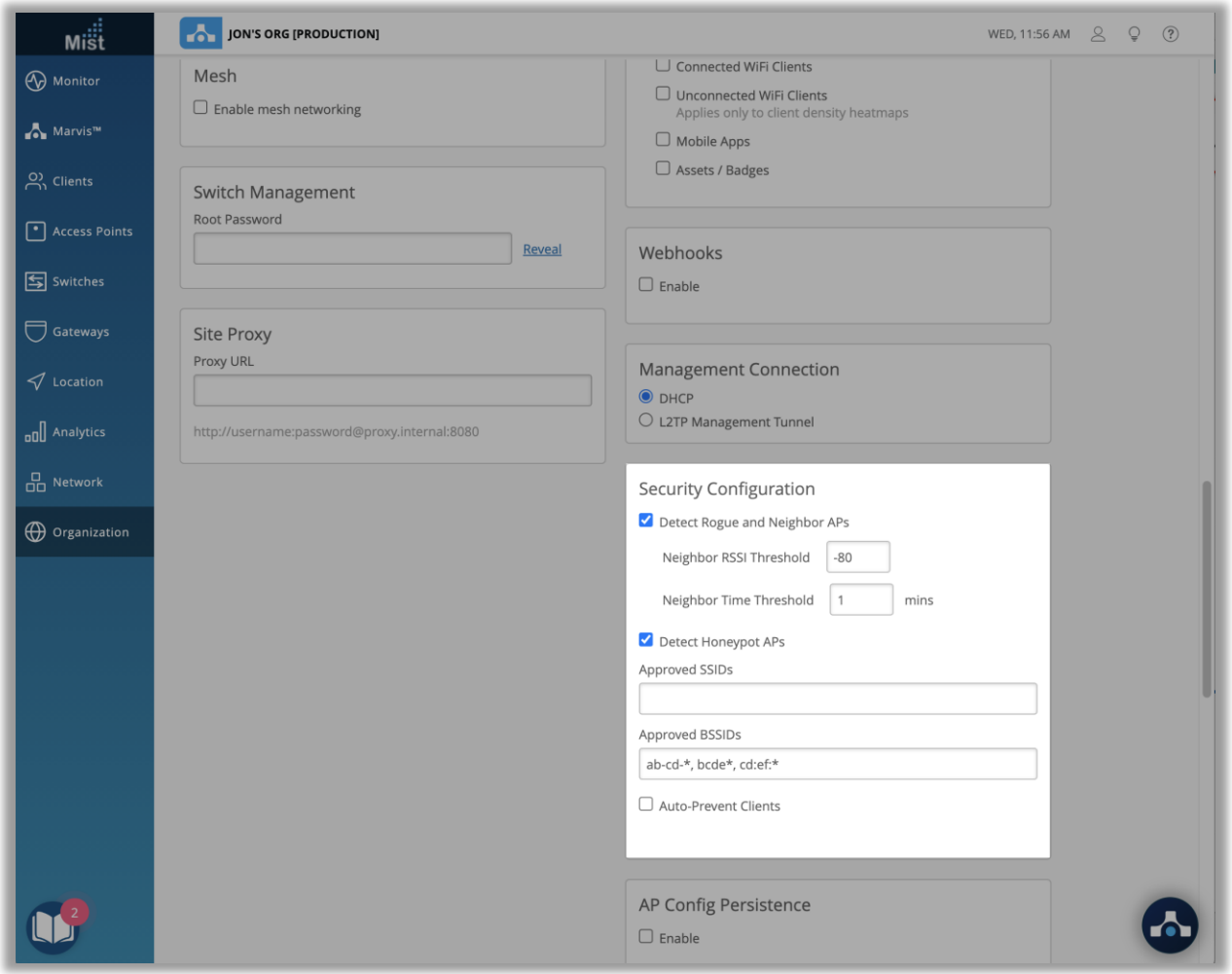
- ここでは、Mistクラウドが正しく動作するためにファイアウォールで有効にする必要のあるポートについて読むことができます。機能やクラウド環境ごとに異なるホスト名とポートを有効にする必要があります

OrganizationのWebhook
監査ログとデバイスステータスログのサポート



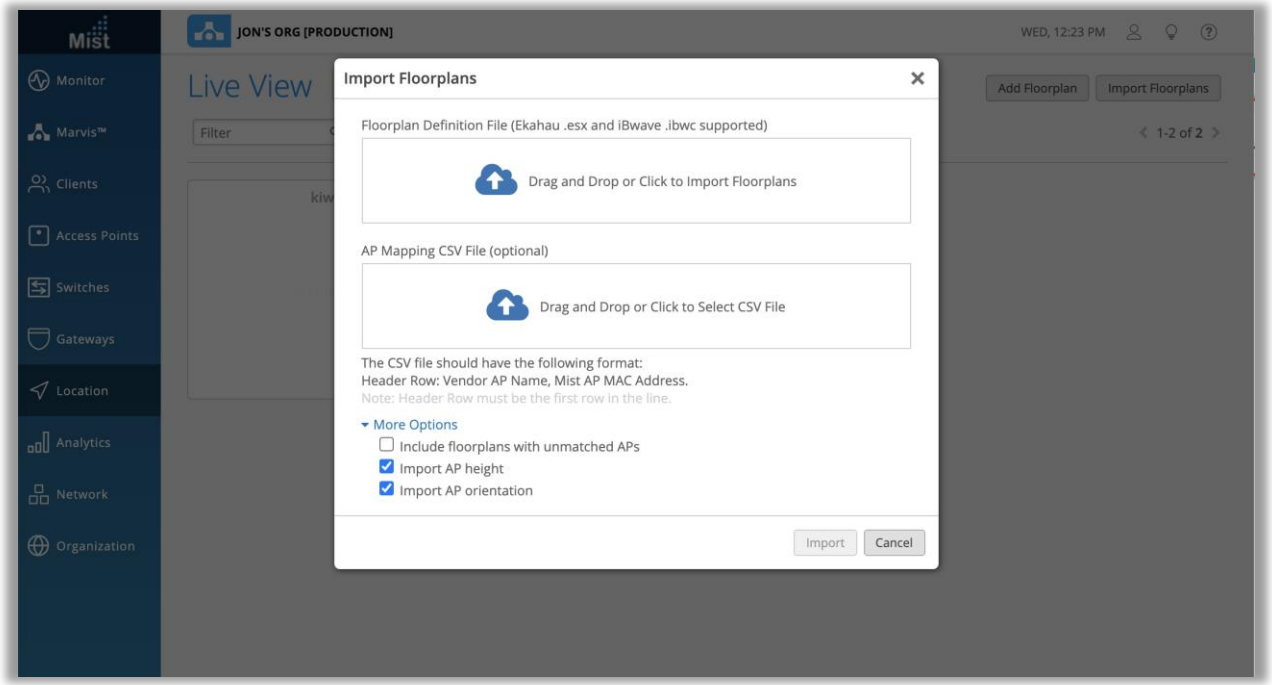
- MistダッシュボードのWebhookを使用して追跡する監査ログとデバイスステータスを含めることで、OrgのWebhook機能を拡張しています
- **[Organization]**ページ（**[Organiation]> [Settings]** ）で、**[Webhook]**セクションの**Audits**チェックボックスと**[Device Status]**チェックボックスを有効にします
- OrganizationのAuditsに表示されるイベント、および再起動イベントやアップグレードなどの発生したデバイスステータスについて、Webhookアラートが表示されます

ネットワークセキュリティー
BSSIDワイルドカード



- ワイルドカードを使用したネットワークセキュリティBSSIDの許可リストの作成をサポートするようになりました
- Rogue / Honeypot AP検出構成でワイルドカードを使用して、特定の文字シーケンスを含むBSSIDを事前承認します
- これらの事前承認されたBSSIDは、セキュリティページに脅威として表示されません。これは、一度に1つのフロアまたは1つの建物でミストに移行する場合に非常に役立ちます
- ワイルドカード機能を使用するには、サイト設定ページ（**[Organization]> [Site settings]** ）に移動し、**[Security configuration]**セクションを見つけます
- ここでは、サイトで承認するBSSIDのセグメントを入力できます。承認されたBSSIDセグメントを次のいずれかの形式で入力します
  - xx-xx-*、xxxx *、xx：xx：*
  - 「*」は、指定された文字が目的のパターンに一致する限り、任意の文字を示します

マップのインポートーデバイスプロファイル

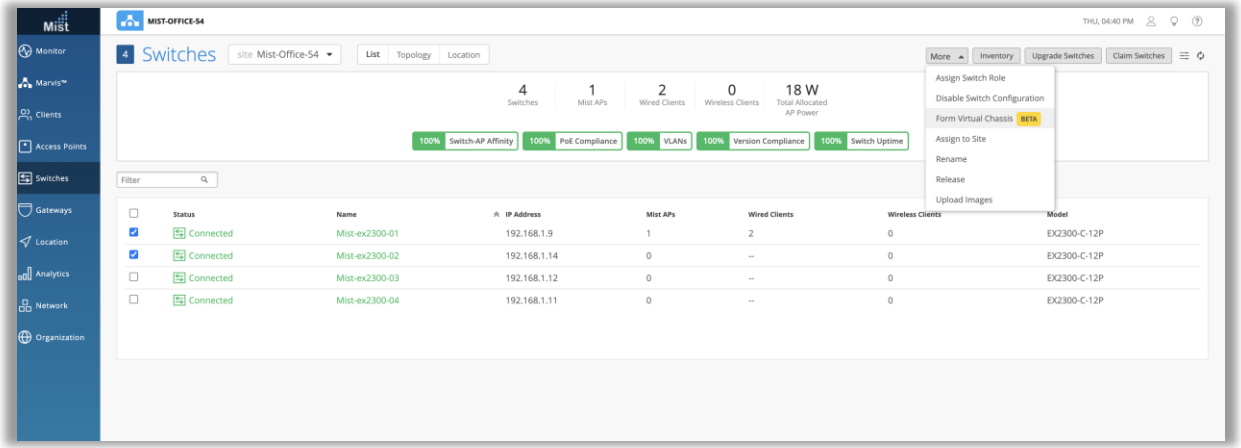


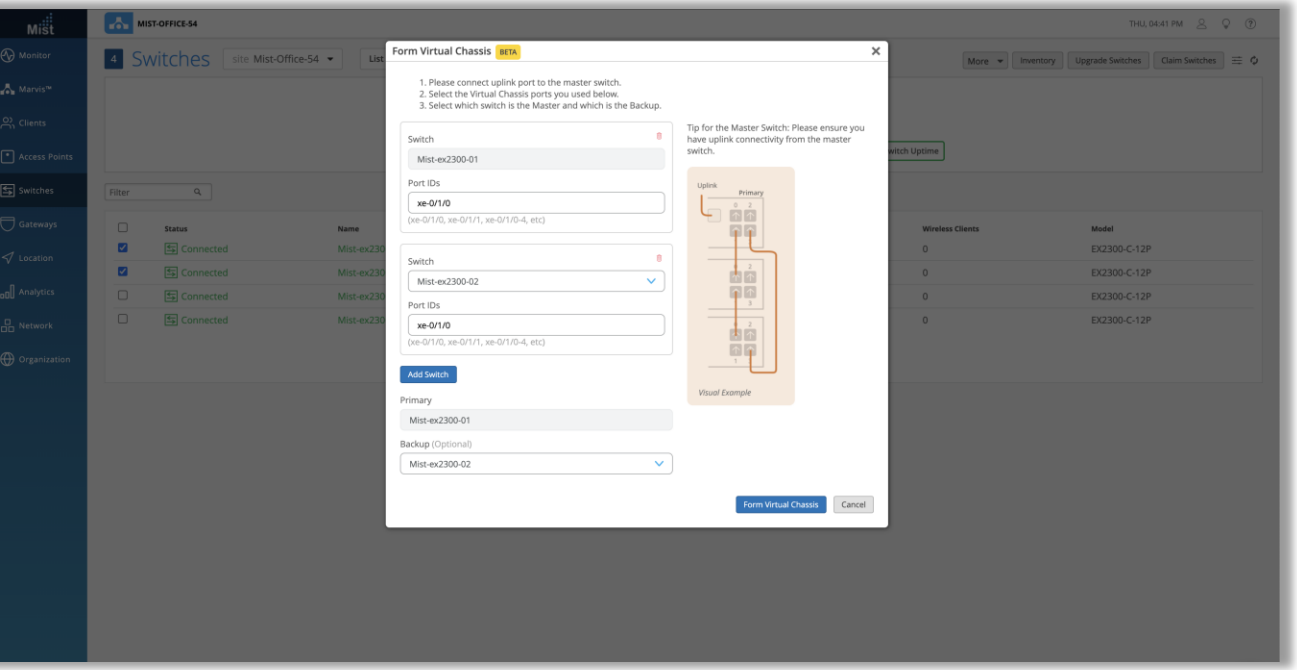
- **(ご注意)現時点では、デバイスプロファイルはGA機能ではないことに注意してください。Organizationでこの機能が必要な場合、またはユースケースについて他に質問がある場合は、support@mist.comまでご連絡ください。**

- Organizationの設定で有効になっている場合の自動デバイスプロファイルのサポートは、マップインポート機能が使用されている場合にサポートされるようになりました
- これにより、新しいサイトでデバイスプロファイル設定を再作成する必要がなくなります。これらは自動的に含まれます。この機能を有効にするために必要なUI設定はないため、フロアプランをインポートするワークフローは同じままです
- フロアプランのインポートについて詳しくは、次のページをご覧ください https://www.mist.com/documentation/importing-ekahau-projects-to-mist/
- デバイスプロファイルの詳細については、次のページをご覧ください https://www.mist.com/documentation/device-profiles/

Wired Assurance

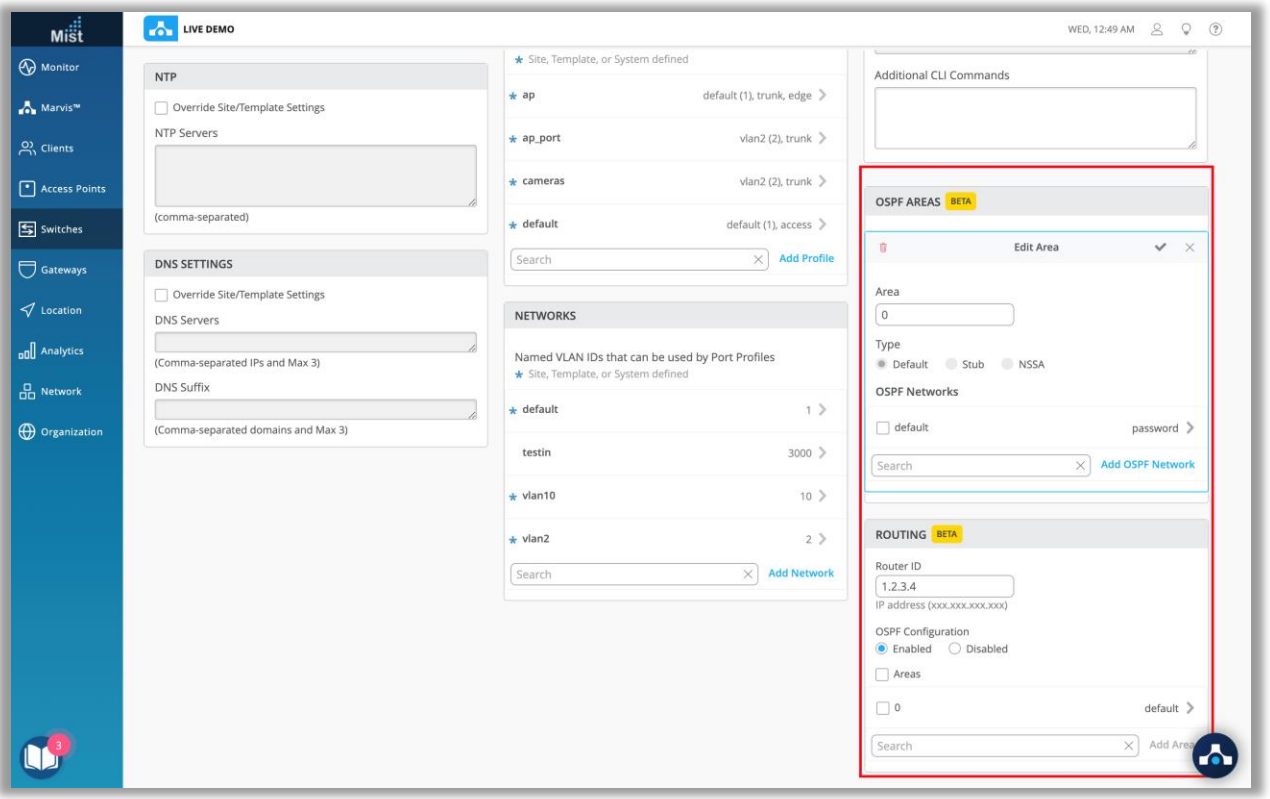
バーチャルシャーシのサポート





- **(ご注意)本設定は専用のVCポートのないEX2300シリーズスイッチにのみ必要であることに注意してください。専用VCポートを備えたスイッチは、ミストクラウドに接続すると自動的にVCを形成します**
- 本リリースでは、SUB-EX *ライセンスを持つすべてのユーザーが利用できる機能としてバーチャルシャーシ（VC）をリリースします
- VCを使用すると、複数のEXスイッチを組み合わせて、ジュニパーミストクラウドに関して単一のデバイスとして機能させることができます
- これにより、ループのリスク、スパニングツリーやVRRPなどのレガシー冗長プロトコルの必要性、および個々のデバイス管理に必要な時間が排除されます
- [**Switch**]ページに移動して目的のスイッチを選択することにより、同じバージョンを実行しているサイトでEX2300シリーズスイッチを使用してVCを簡単に形成できます
- 両方がクラウドにも接続されていることを確認してください。[**More**]ドロップダウンメニューを使用して、[**Form Virtual Chassis**]を選択して手順を開始できます

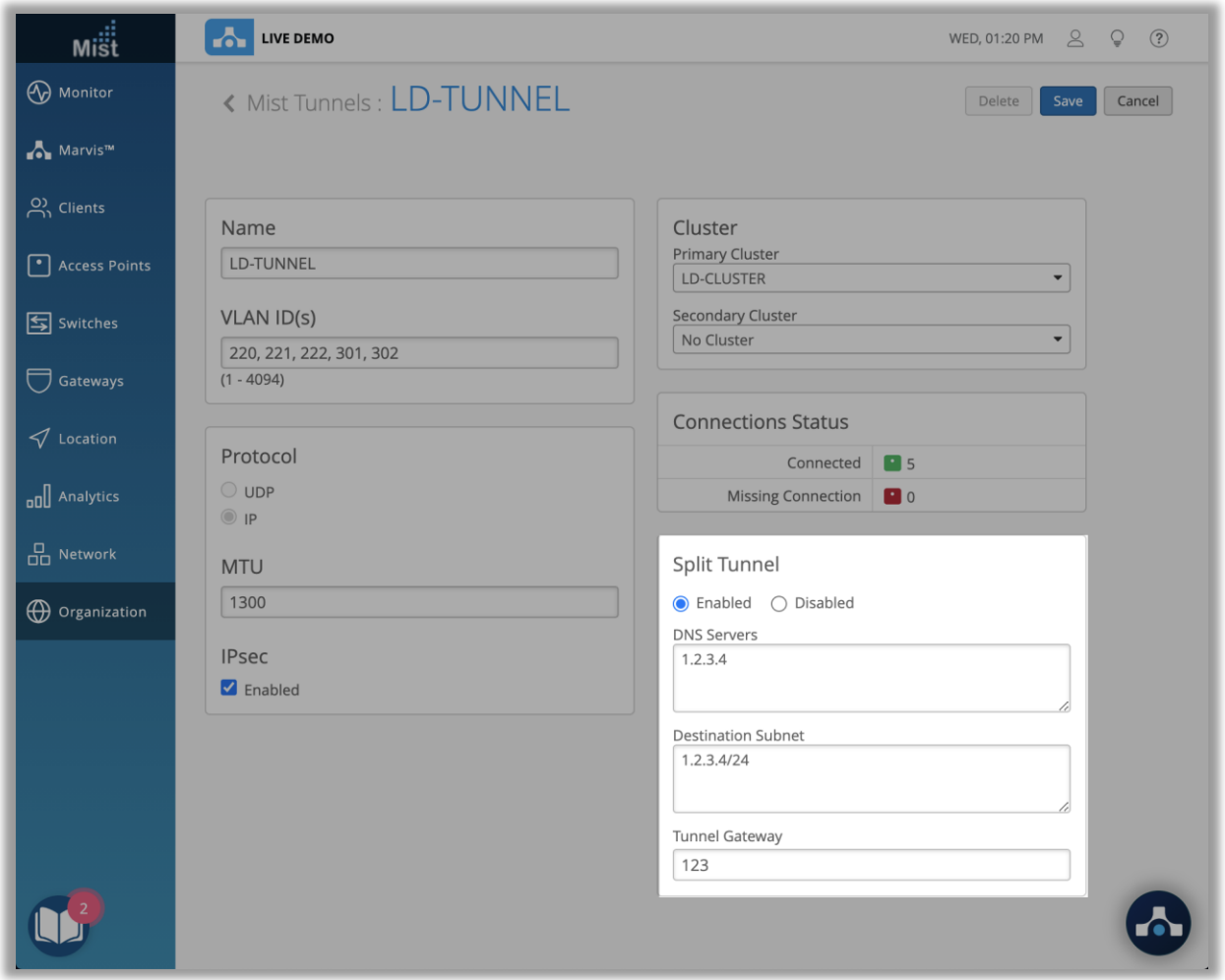
OSPF エリアとルーティングの設定[ベータ]



- 本リリースでは、ベータ機能として、OSPF(Open Shortest Path First)のAreaとRoutingの設定をUIでサポートします
- OSPF Areasでは、スイッチが属するエリアと、そこに属するネットワークを定義し、Routingでは、ルーターIDの定義と、これらのエリアのOSPF設定の切り替えを行います
- OSPFを設定するには、Switch Detailsページ（Switch > Select a Switch)をご参照ください

Mist Edge

スプリットトンネル



- 自宅でのリモートワークに必要なスプリットトンネル機能を、SUB-MEライセンスをお持ちのすべてのユーザーに提供します
- スプリットトンネルは、特定の一致する宛先のみをミストエッジにトンネリングし、残りのリモートユーザーのトラフィックは自宅のブロードバンドを経由して通信します
- これにより、リモートユーザーのトラフィック全体をトンネリングしないことで、DCやDMZのネットワーク帯域を節約することができます
- Mist Edgeにスプリットトンネルを設定するには、「Organization」>「Mist Tunnel」に移動し、「Split Tunnel」で「Enabled」を選択します。ここでは、DNS サーバー、サブネット、およびトンネルゲートウェイを指定する必要があります
- 詳細については、Mist Teleworker Guide を参照してください https://www.mist.com/documentation/mist-edge-configuration-guides/


Thank you
JUNIPER
driven by Mist AI