

# 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

The screenshot shows the Marvis AI dashboard interface. At the top, there's a navigation bar with 'MIST CSQA MIST OFFICE' and 'MARVIS'. The main area features a central 'ACTIONS' hub with a count of 22. Below this hub, there are several categories: '0 Clients', '1 Layer 1', '4 Connectivity', '8 AP', '7 Switch', '2 Gateways', 'Application', and 'Security'. A red box highlights the '2 Other Actions' section, which is linked to '2 Persistently Failing Clients'. Below this, there's a 'PERSISTENTLY FAILING' section with a 'RECOMMENDED ACTION' and a table of failing clients.

Site	Clients	Details	Date
Wired Assurance	3 Clients	PSK Failed <a href="#">View More</a>	Jun 27, 2021 12:57 AM
Wired Assurance	3 Clients	802.1x Auth Fail <a href="#">View More</a>	Jun 25, 2021 08:58 PM

- “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

The screenshot shows the Juniper Mist Marvis interface. A network diagram is visible in the background, showing a hierarchy from Layer 1 to APs and Switches. A popup window titled 'Persistently Failing Details' is open, displaying the following information:

Client Name	MAC Address	WLAN
Kush_1	2d:93:43:31:40:8f	WLAN: AP43_WLAN.
Kush_2	89:3d:7f:da:79:94	WLAN: Carrefour2.
Kush_3	13:55:fc:7f:eb:4c	WLAN: ISE-Guest-AP43.

Below the popup, the 'Persistently Failing' section shows a table of failed clients:

Site	Clients	Details	Date
<input type="checkbox"/> Wired Assurance	3 Clients	PSK Failed <a href="#">View More</a>	Jun 27, 2021 12:57 AM
<input type="checkbox"/> Wired Assurance	3 Clients	802.1x Auth Fail <a href="#">View More</a>	Jun 25, 2021 08:58 PM

- **[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

The screenshot displays the Mist Marvis dashboard interface. At the top, it shows the user's location as 'MIST CSQA MIST OFFICE' and the time 'WED, 05:32 PM'. The main navigation menu on the left includes Monitor, Marvis, Clients, Access Points, Switches, Gateways, Location, Analytics, Network, and Organization. The central 'ACTIONS' section shows a tree view with 22 total actions, categorized into Clients (0), Layer 1 (1), Connectivity (4), AP (8), Switch (7), Gateways (2), Security, and Application. A list of reasons for the 'Switch' category is shown, with 'Port Flap' highlighted in a red box. Below this, the 'PORT FLAP' section provides a 'RECOMMENDED ACTION' and a table of affected devices.

Site	Switch	Details	Date
Wired Assurance	Abhi_1	2 Ports <a href="#">View More</a>	Jun 26, 2021 08:51 PM

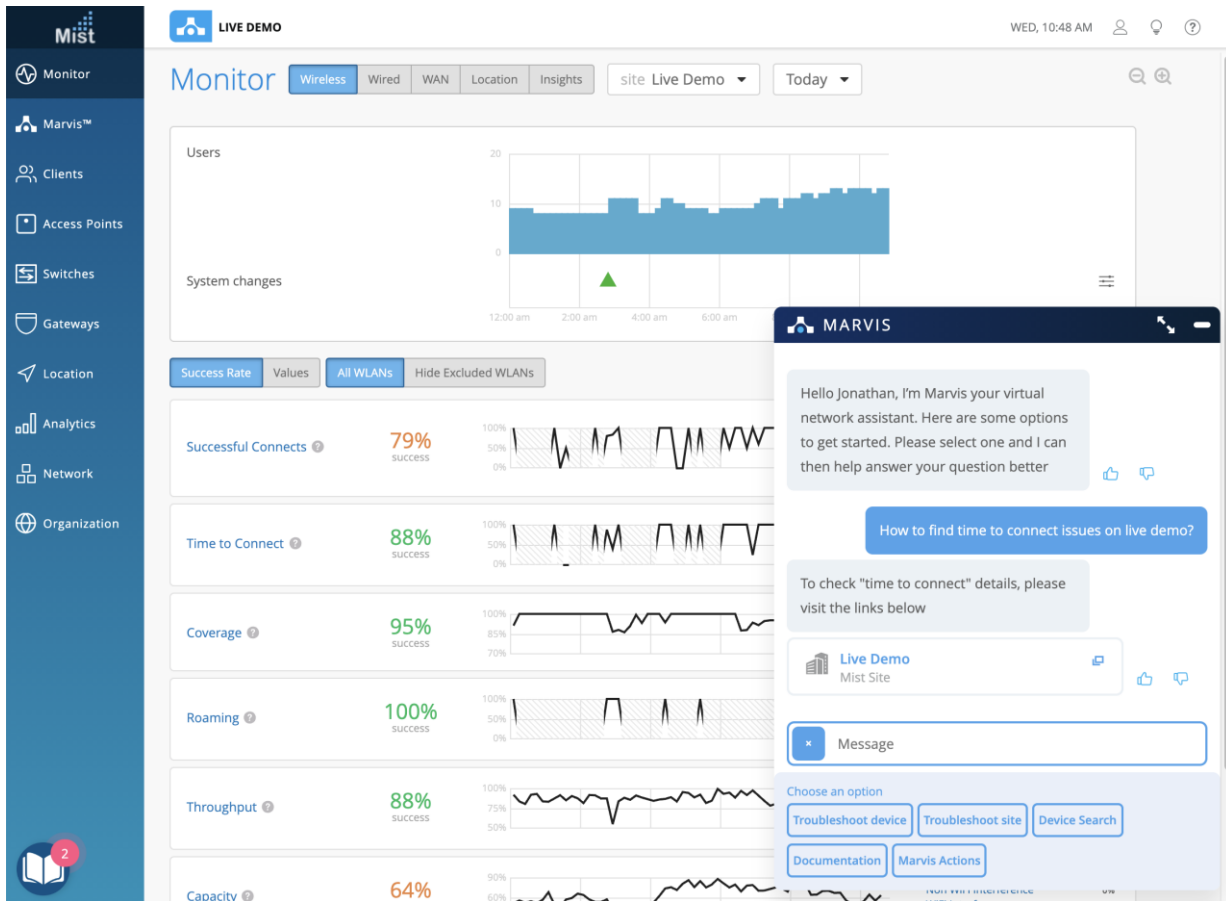
- ポートフラップは、アクションダッシュボードの[Switch]セクションで使用できる新しいアクションです
- このアクションにより、さまざまな理由で継続的にアップおよびダウンしているスイッチのポートが識別されます
- ポートのフラッピングは、接続の信頼性の低さ、ポートに接続されているデバイスの継続的な再起動、不適切なデュプレックス構成などが原因である可能性があります

# 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

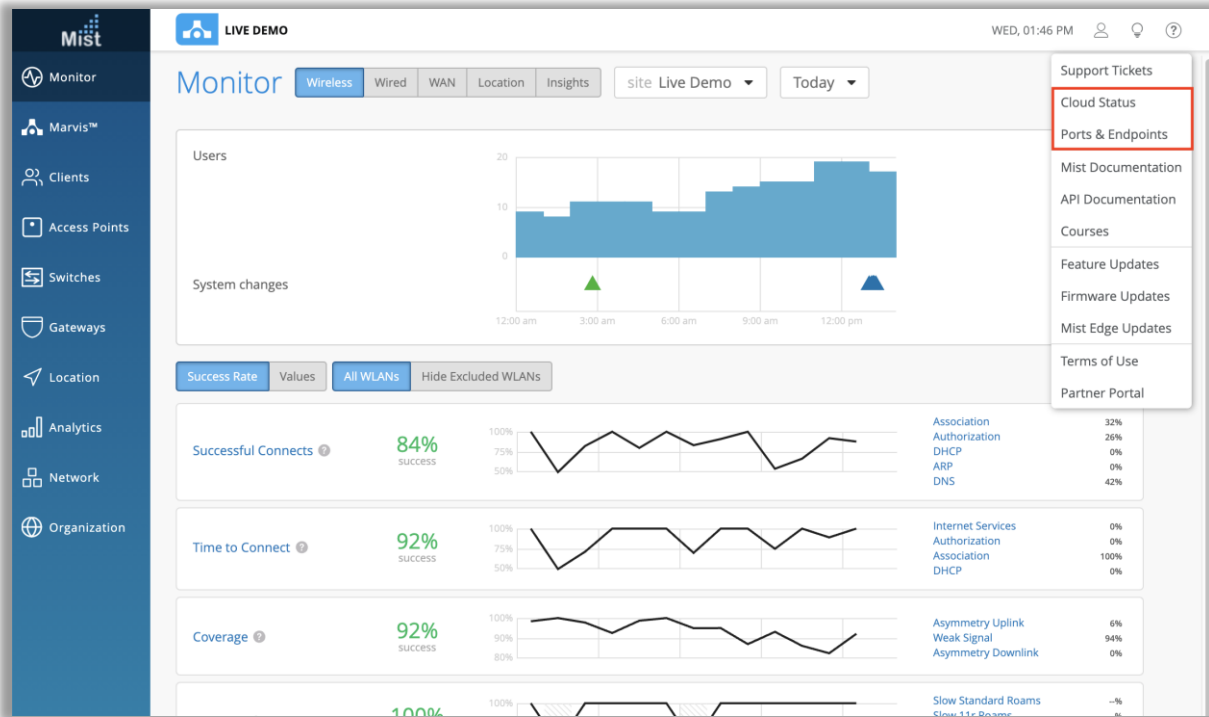
例：“How to find time to connect issues at <name>”  
では、Time to Connect SLEのUIに移動します





# 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

MIST CLOUD STATUS

Get Updates via Slack or Email

- Email  
Updates to your Email
- Slack  
Live updates to a #channel of your choice

MIST CLOUD STATUS

Questions? [Contact Support](#)

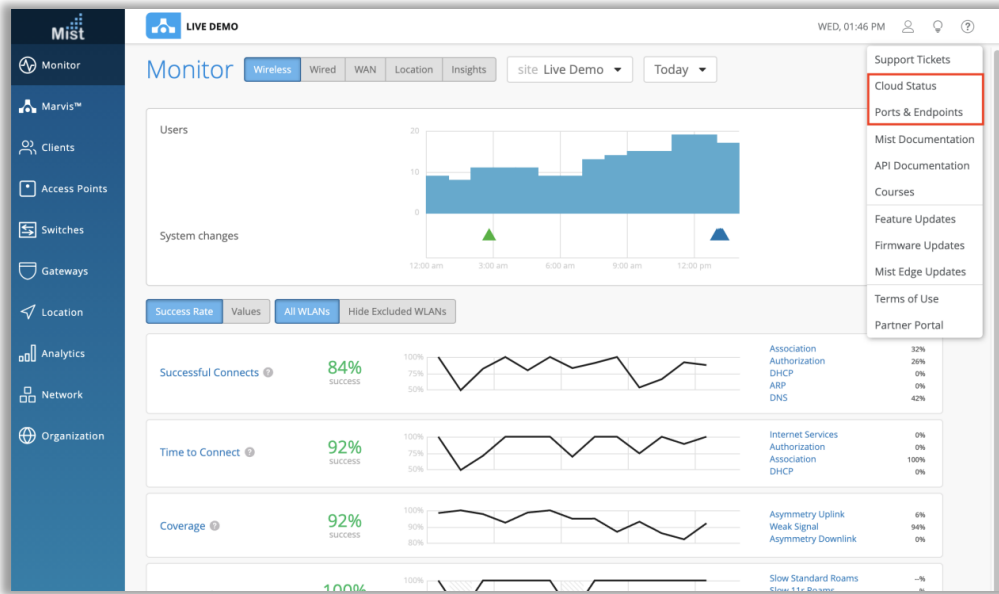
MIST GLOBAL CLOUD	Operational
MIST EUROPE CLOUD	Operational

Previous Incidents

No further notices from the past 7 days.

- 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

2021 Gartner Magic Quadrant for Indoor Location Services, Global [Get Report](#)

**JUNIPER**  
driven by Mist AI

## Ports to enable on your firewall

**Mist Cloud**

Service Type	Global 01	Global 02	Europe 01
Admin Portal	admin.mist.com (TCP 443) api.wi.mist.com (TCP 443) api.wireless.com (TCP 443)	admin.g1.mist.com (TCP 443) api.wi.eu.mist.com (TCP 443) api.wireless.com (TCP 443)	admin.eu.mist.com (TCP 443) api.wi.eu.mist.com (TCP 443) api.wireless.com (TCP 443)
Guest Wi-Fi Portal	portal.mist.com (TCP 443)	portal.g1.mist.com (TCP 443)	portal.eu.mist.com (TCP 443)
Workbooks source IP Addresses	54.193.71.17 54.211.237.20	54.94.120.8 51.236.34.24 51.236.92.224	51.133.173.223 51.121.19.146 51.120.165.1

**Device to Mist Cloud Communication:**

Device Type	Global 01	Global 02	Europe 01
Mist AP / Mist Edge	api.terminator.mist.com (TCP 443) portal.mist.com (TCP 443)	api.terminator.mist.com (TCP 443) portal.g1.mist.com (TCP 443)	api.terminator.mist.com (TCP 443) portal.eu.mist.com (TCP 443)
EX Switch	redfish.juniper.net (TCP 443) api.mist.com (TCP 443) api.terminator.mist.com (TCP 2200)	redfish.juniper.net (TCP 443) api.g1.mist.com (TCP 443) api.terminator.mist.com (TCP 2200)	redfish.juniper.net (TCP 443) api.eu.mist.com (TCP 443) api.terminator.mist.com (TCP 2200)
SRX Gateway	redfish.juniper.net (TCP 443) api.terminator.mist.com (TCP 2200) api.log.terminator.mist.com (TCP 8314)	redfish.juniper.net (TCP 443) api.g1.mist.com (TCP 443) api.terminator.mist.com (TCP 2200) api.log.terminator.g1.mist.com (TCP 8314)	redfish.juniper.net (TCP 443) api.eu.mist.com (TCP 443) api.terminator.mist.com (TCP 2200) api.log.terminator.eu.mist.com (TCP 8314)

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

The screenshot displays the Mist Management Console interface for an organization named 'JON'S ORG (PRODUCTION)'. The left sidebar contains navigation options: Monitor, Marvis™, Clients, Access Points, Switches, Gateways, Location, Analytics, Network, and Organization. The main content area is divided into several sections: Managed Service Provider (none), Password Policy (Enabled), Session Policy (20160 minutes), Auto-Provisioning, Site Assignment (Disabled), AP Name Generation (Disabled), Device Profile Assignment (Disabled), Support Access (checked), Mist Certificate, RadSec Certificates, AP RadSec Certificate, CloudShark Integration, Roles, Security (checked), and Webhooks. The Webhooks section is highlighted, showing the following configuration: Enable (checked), Name: org\_webhook, URL: https://enqnpipb38rxl.x.pipedream.net/, Secret (empty), and Streaming API (Alerts unchecked, Audits checked, Device Status checked).

- 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 (**[Organization]**> **[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

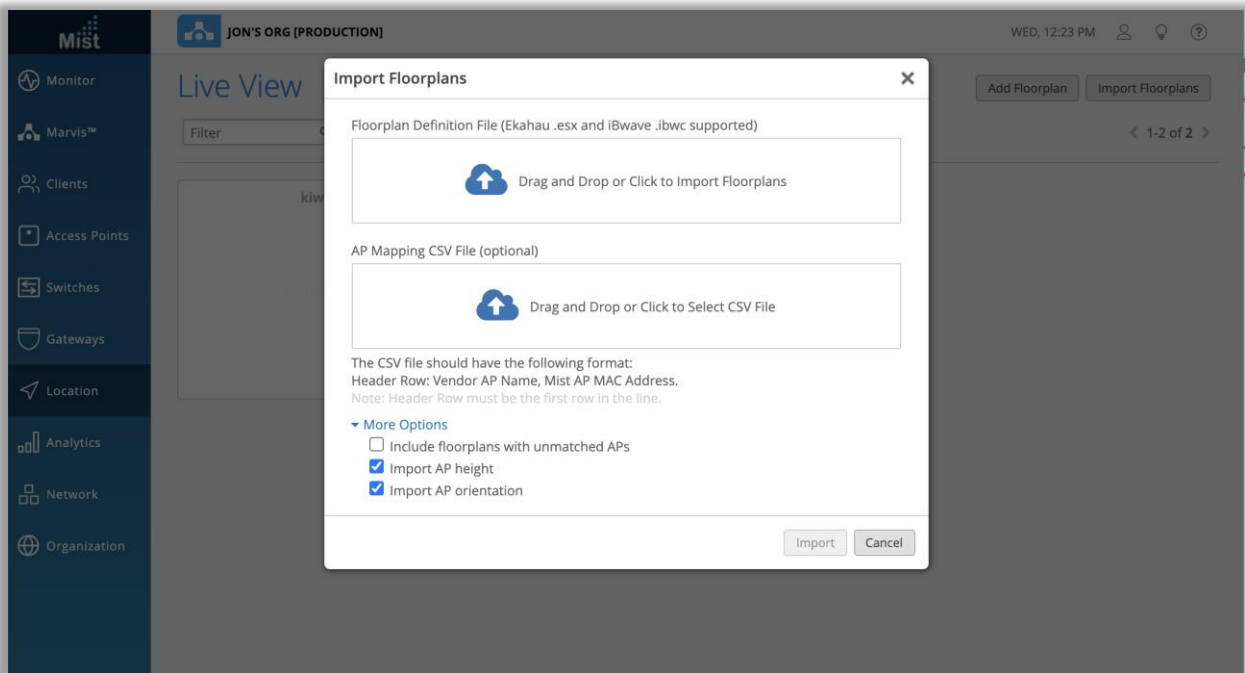
# ネットワークセキュリティ BSSIDワイルドカード

The screenshot shows the Mist Management Console interface for 'JON'S ORG [PRODUCTION]'. The 'Security Configuration' section is highlighted, showing the following settings:

- Detect Rogue and Neighbor APs
  - Neighbor RSSI Threshold: -80
  - Neighbor Time Threshold: 1 mins
- Detect Honeypot APs
  - Approved SSIDs: [Empty field]
  - Approved BSSIDs: ab-cd-\*, bcde\*, cd:ef:\*
- Auto-Prevent Clients

- 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-デバイスプロフィール

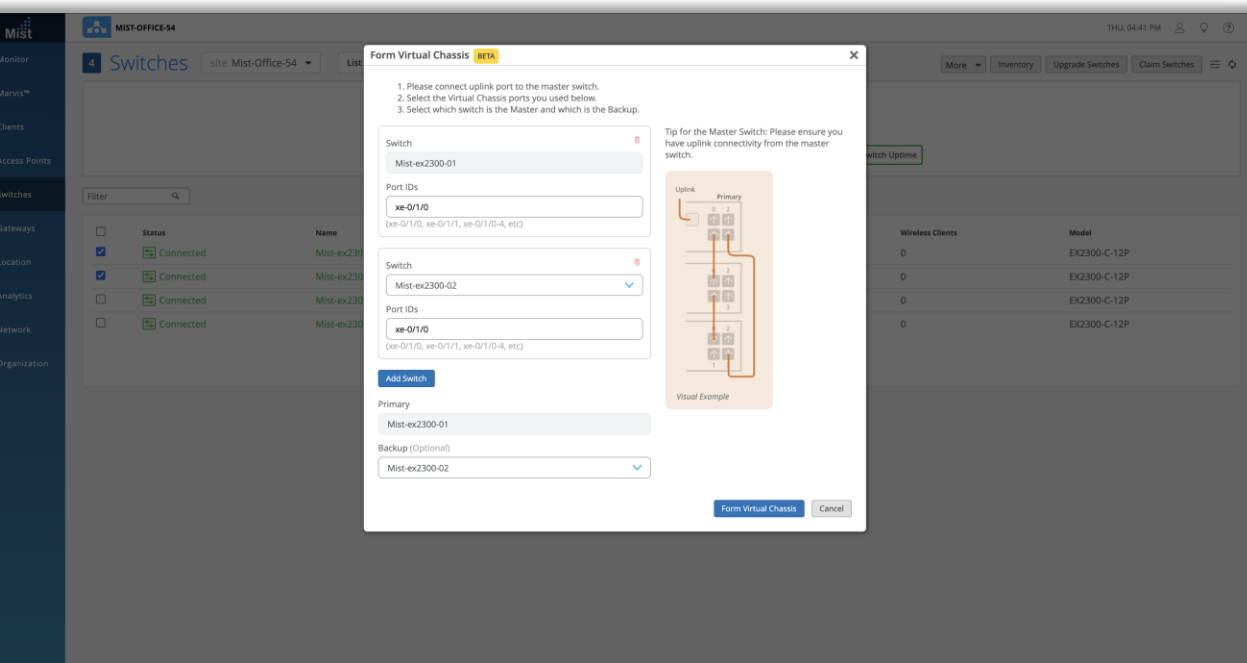
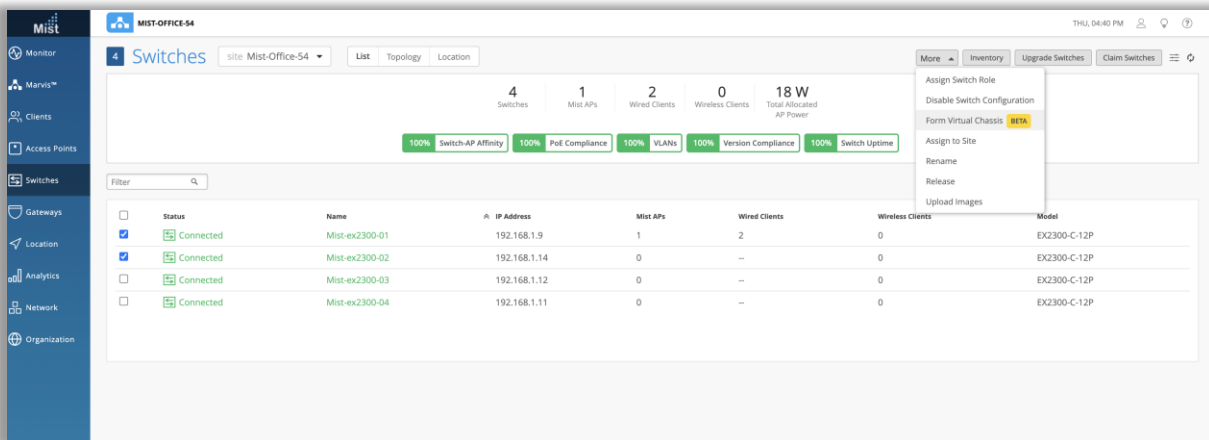


- (ご注意)現時点では、デバイスプロフィールはGA機能ではないことに注意してください。Organizationでこの機能が必要な場合、またはユースケースについて他に質問がある場合は、[support@mist.com](mailto:support@mist.com)までご連絡ください。
- Organizationの設定で有効になっている場合の自動デバイスプロフィールのサポートは、マップインポート機能が使用されている場合にサポートされるようになりました
- これにより、新しいサイトでデバイスプロフィール設定を再作成する必要がなくなります。これらは自動的に含まれます。この機能を有効にするために必要な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/>
- デバイスプロフィー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、スパンニングツリーや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]

The screenshot displays the Mist management console interface. On the left is a navigation sidebar with icons for Monitor, Marvis, Clients, Access Points, Switches, Gateways, Location, Analytics, Network, and Organization. The main content area is divided into several sections: 'NTP' with an 'Override Site/Template Settings' checkbox and an input field for 'NTP Servers'; 'DNS SETTINGS' with an 'Override Site/Template Settings' checkbox and input fields for 'DNS Servers' and 'DNS Suffix'; and 'NETWORKS' with a table of VLANs. The 'NETWORKS' table lists 'default' (1), 'testin' (3000), 'vlan10' (10), and 'vlan2' (2). A red box highlights the 'OSPF AREAS BETA' configuration panel, which includes an 'Edit Area' dialog with fields for 'Area' (set to 0), 'Type' (Default, Stub, or NSSA), and 'OSPF Networks' (with a 'default' entry and a 'password' field). Below this is the 'ROUTING BETA' section with a 'Router ID' field (set to 1.2.3.4), 'OSPF Configuration' (Enabled/Disabled), and 'Areas' (with a '0' entry).

- 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

The screenshot displays the Mist Edge configuration page for a tunnel named 'LD-TUNNEL'. The interface includes a sidebar with navigation options like Monitor, Marvis, Clients, Access Points, Switches, Gateways, Location, Analytics, Network, and Organization. The main configuration area is divided into several sections: Name (LD-TUNNEL), VLAN ID(s) (220, 221, 222, 301, 302), Protocol (IP selected), MTU (1300), IPsec (Enabled), Cluster (LD-CLUSTER), and Split Tunnel settings (Enabled, DNS Servers: 1.2.3.4, Destination Subnet: 1.2.3.4/24, Tunnel Gateway: 123). A 'Connections Status' table shows 5 connected and 0 missing connections.

- 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

