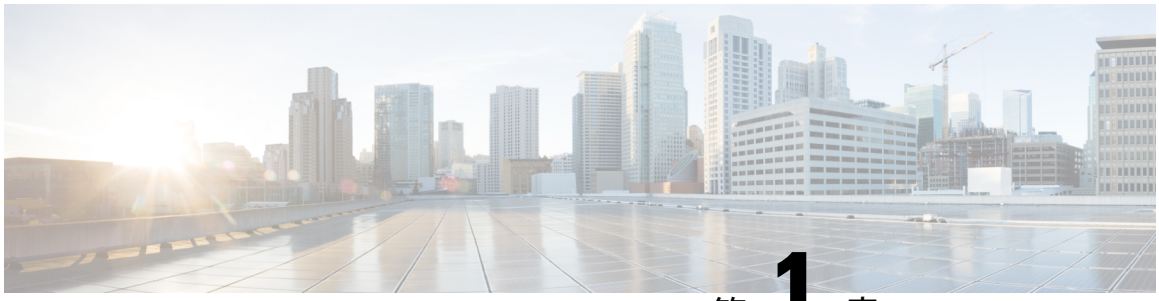
Cisco Secure Malware Analytics アプライアンス管理者ガイド バージョン 2.19

最終更新：2025 年 4 月 30 日

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/

【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。

目 次



第 1 章

はじめに

Cisco Secure Malware Analytics Appliance アドミニストレーション ガイド へようこそこの章では、アプライアンスの概要、対象読者、および関連する製品マニュアルへのアクセス方法について説明します。

Secure Malware Analytics アプライアンスについて

Secure Malware Analytics アプライアンスは、詳細な脅威分析およびコンテンツ分析を使用して、安全性に優れたオンプレミスの高度なマルウェア分析を提供します。Cisco Secure Malware Analytics アプライアンスは、完全なマルウェア分析プラットフォームを提供し、Cisco Secure Malware Analytics M6 Applicance server（v.2.19 以降）またはM5 アプライアンスサーバー（v2.7.2 以降）にインストールされます。さまざまなコンプライアンスおよび Secure Malware Analytics ポリシーの制限に基づいて運営されている組織が、マルウェアサンプルをアプライアンスに送信できるようにします。

（注） Cisco UCS C220 M4（TG5400）サーバーは、Cisco Secure Malware Analytics アプライアンスで引き続きサポートされていますが、サーバーのサポートは終了しています。

銀行や医療サービスなどの機密データを扱う組織の多くは、マルウェアアーティファクトといった特定の種類のファイルをマルウェア分析のためにネットワーク外に送信することを許可しない、さまざまな規制ルールおよびガイドラインに従う必要があります。Cisco Secure Malware Analytics アプライアンスをオンプレミスで維持することにより、組織はネットワークを離れることなく、疑わしいドキュメントやファイルを分析対象として送信できます。

Cisco Secure Malware Analytics アプライアンスを使用することで、セキュリティチームは非常にセキュアな独自の静的および動的分析テクニックを使用し、すべてのサンプルを分析できるようになります。アプライアンスでは、分析結果を数億もの分析済みマルウェアアーティファクトと関連付け、マルウェア攻撃、キャンペーン、およびその配布状況をグローバルに把握できるようにします。観測された 1 つの活動/特性サンプルを他の数百万ものサンプルとすみやかに関連付け、比較することで、過去の履歴やグローバルなコンテキストに照らして、その動作を十分に理解できます。この機能は、高度なマルウェアからの脅威と攻撃に対して、セキュリティ チームが効果的に組織を守るために役立ちます。

このリリースの最新情報

バージョン 2.19 のこのガイドでは、次の変更が行われました。

表 *1:* バージョン *2.19* における変更

機能または更新	セクション
ファームウェアの更新	FirmwareUp によるファームウェアの更新 （165 ページ）
管理 UI のダッシュボードの機能強化	ホーム （57 ページ）
TGSH では、クリーンおよびダーティインターフェイスを介して ping を実行できるようになりました。	-

対象読者

このガイドは、アプライアンスのセットアップと設定が完了し、最初のテストマルウェアサンプルが正常に送信および分析された後に、Cisco Secure Malware Analytics アプライアンス管理者が使用することを目的としています。マルウェア分析ツール、アプライアンスの更新、バックアップ、その他のサーバー管理タスクに関して、組織とユーザーを管理する方法について説明します。

さらに、Cisco Secure Malware Analytics アプライアンスと他のシスコ製品やサービス（Cisco E メールセキュリティアプライアンス、Cisco Web セキュリティアプライアンス、Secure Endpoint プライベートクラウドデバイスなど）を統合する管理者に向けた情報も提供します。

（注） Cisco Secure Malware Analytics アプライアンスのセットアップと構成の詳細については、『*Cisco Threat Grid Getting Started Guide*』を参照してください。

このマニュアルについて

このガイドには、計画に関する情報、設定作業、および一般的な管理タスクが記載されています。構成は次のとおりです。

章	説明
はじめに	アプライアンスの簡単な説明、対象読者、関連する製品マニュアルへのアクセス方法、ログイン名とパスワード、管理者パスワードのリセット方法、サポートへの連絡を提供します。
計画	セットアップと構成の前に確認する必要がある環境、ハードウェア、およびネットワークの要件について説明します。
ネットワーク	管理 TUI を使用した初期ネットワーク設定の変更、管理 TUI への再接続、およびリカバリモードでのネットワークの設定に関する情報を提供します。
ホーム （57 ページ）	管理 UI のホーム画面の使用に関する情報を提供します。
構成	管理 UI を使用してアプライアンスの設定を変更することについての情報を提供します。
ステータス	インストールされているシステムパッケージとそのバージョン、詳細ログ、使用可能なストレージなど、管理 UI でのシステム情報の表示に関する情報を提供します。
操作	設定変更のアクティブ化、管理 UI のリロード、ジョブと電力設定の管理、および更新のインストールに関する情報を提供します。
サポート	アプライアンスの問題の解決を支援するために、ライブ サポート セッションを開始し、サポート スナップショットを作成する手順を示します。
組織およびユーザー	組織の作成、ユーザーの管理、新しいデバイス ユーザー アカウントのアクティブ化の手順を説明します。
インバウンドおよびアウトバウンド接続	他の Cisco アプライアンス（ESA および WSA）および Cisco Secure Endpoint プライベートクラウドを Cisco Secure Malware Analytics アプライアンスに接続する方法について説明します。
アプライアンスのワイプ操作によるすべてのデータの削除	アプライアンスのワイプオプションを使用して、クラスタを含む Cisco Secure Malware Analytics アプライアンスからすべてのデータを削除する方法について説明します。
FirmwareUp によるファームウェアの更新（165 ページ）	ファームウェアの更新方法について説明します。

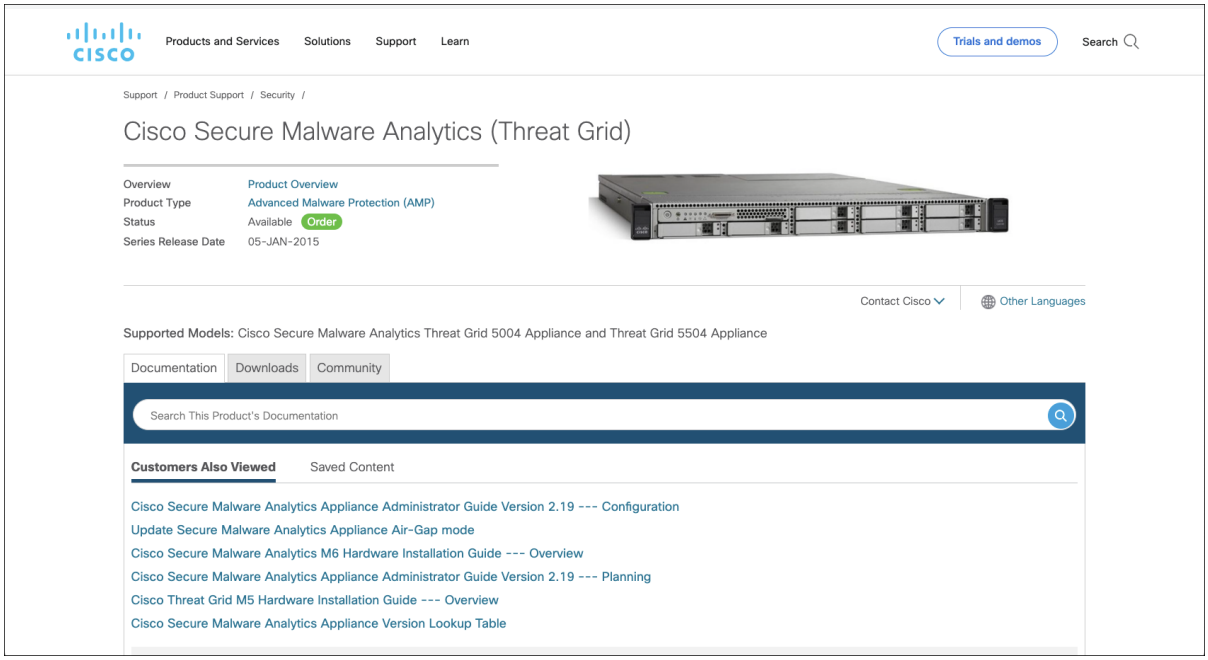
章	説明
CIMC の設定	CIMC ユーティリティを使用してリモート サーバー管理を設定する方法について説明します。

ユーザーマニュアル

Cisco Secure Malware Analytics アプライアンスのユーザーマニュアル

Cisco Secure Malware Analytics アプライアンス製品に関する資料の最新バージョンは、Cisco.com から入手できます。

図 *1 : cisco.com* のユーザーガイド



- *Cisco Secure Malware Analytics Appliance Release Notes*
- *Cisco Secure Malware Analytics アプライアンス v2.19 スタートアップガイド*
- *Cisco Secure Malware Analytics Version Lookup Table*
- *Cisco Secure Malware Analytics M6 Hardware Installation Guide*

（注） Cisco Secure Malware Analytics M6 アプライアンスは、アプライアンス バージョン 2.19 以降でサポートされています。

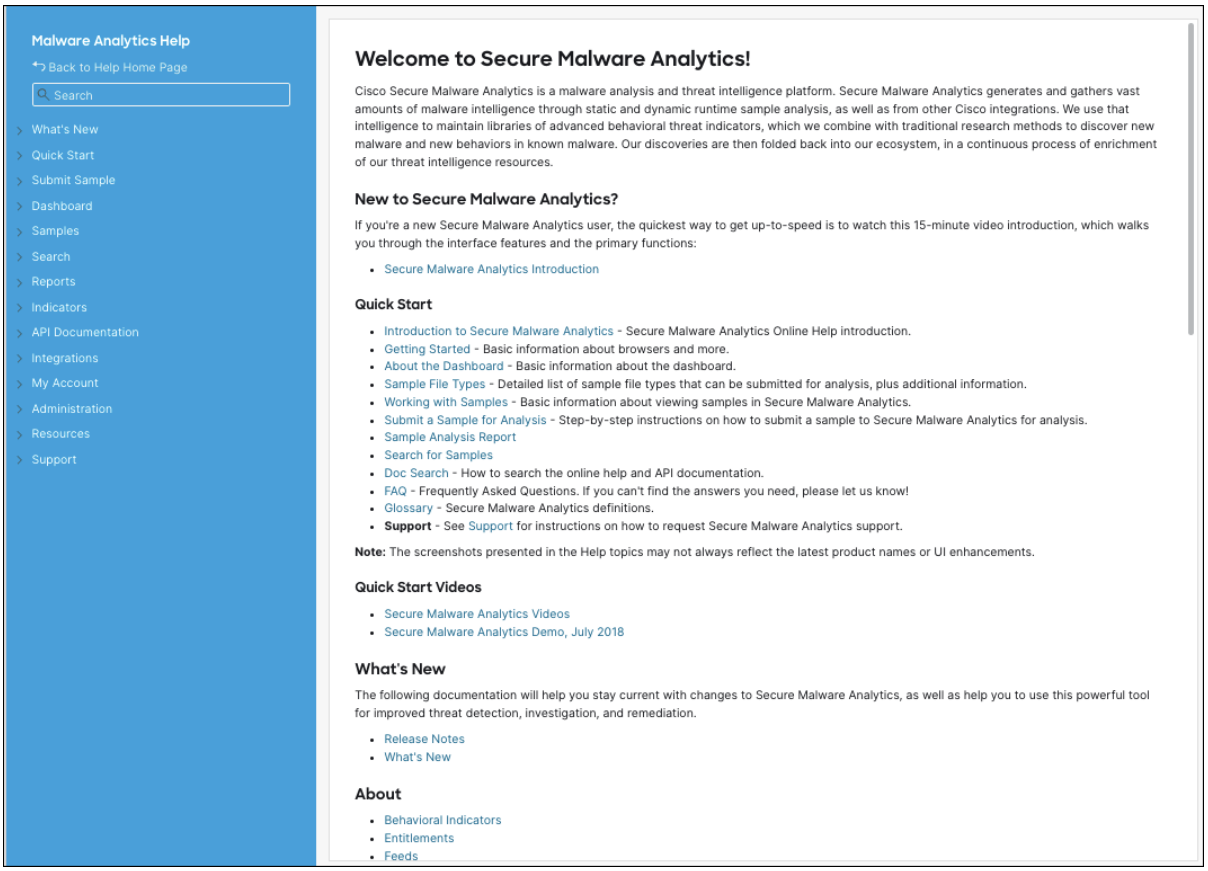
- *Cisco Secure Malware Analytics M5 Hardware Installation Guide*

（注） Cisco Secure Malware Analytics M5 アプライアンスは、アプライアンス バージョン 2.7.2 以降でサポートされています。

Cisco Secure Malware Analytics ポータル UI オンラインヘルプ

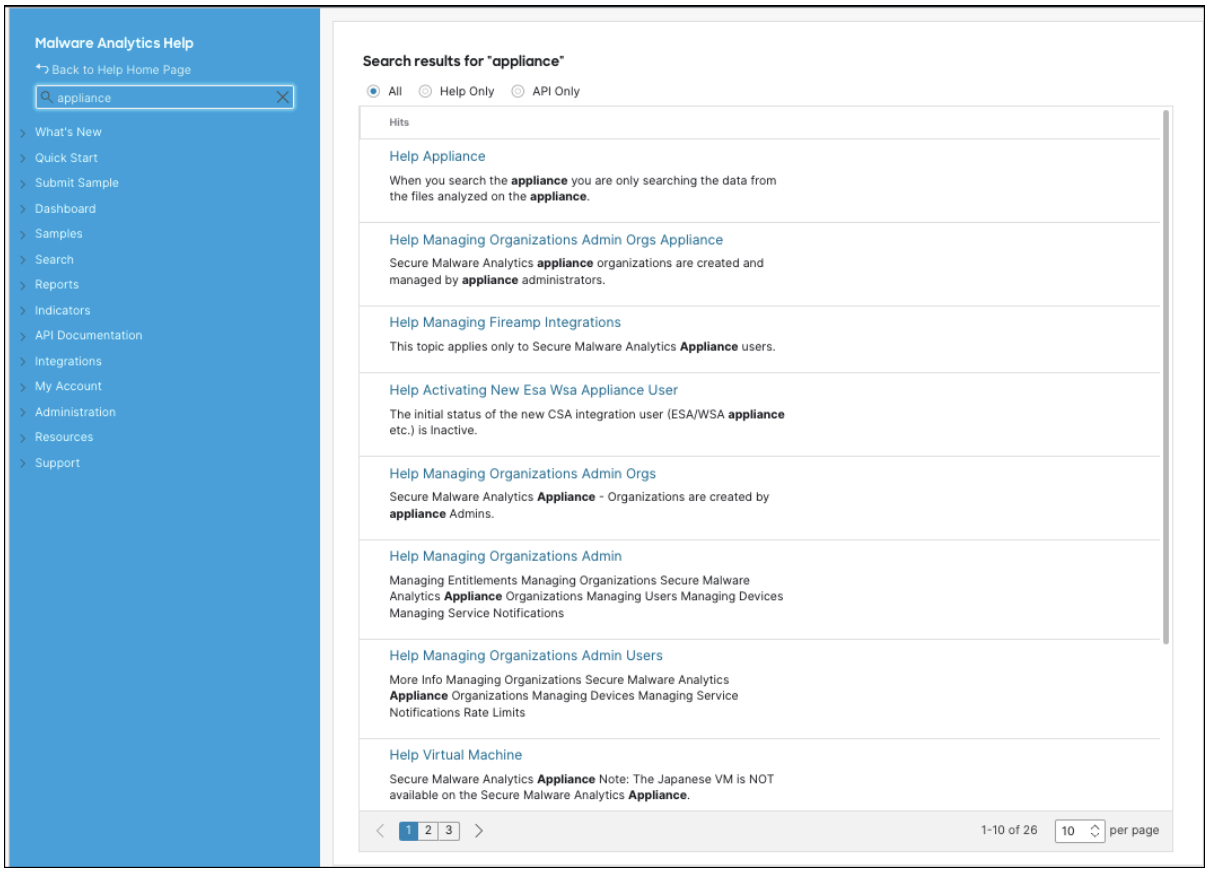
リリースノート、Cisco Secure Malware Analytics オンライン ヘルプ、API ドキュメント、およびその他の情報を含む Cisco Secure Malware Analytics ポータル ユーザー ドキュメントはCisco Secure Malware Analytics ユーザーインターフェイスの右上隅にあるナビゲーションバーにある **[?（ヘルプ）]** アイコンから入手できます。

図 *2 : Cisco Secure Malware Analytics* ポータル オンライン ヘルプ



左列の上部にあるオンラインヘルプの検索機能を使用して、アプライアンス固有の情報を検索します。

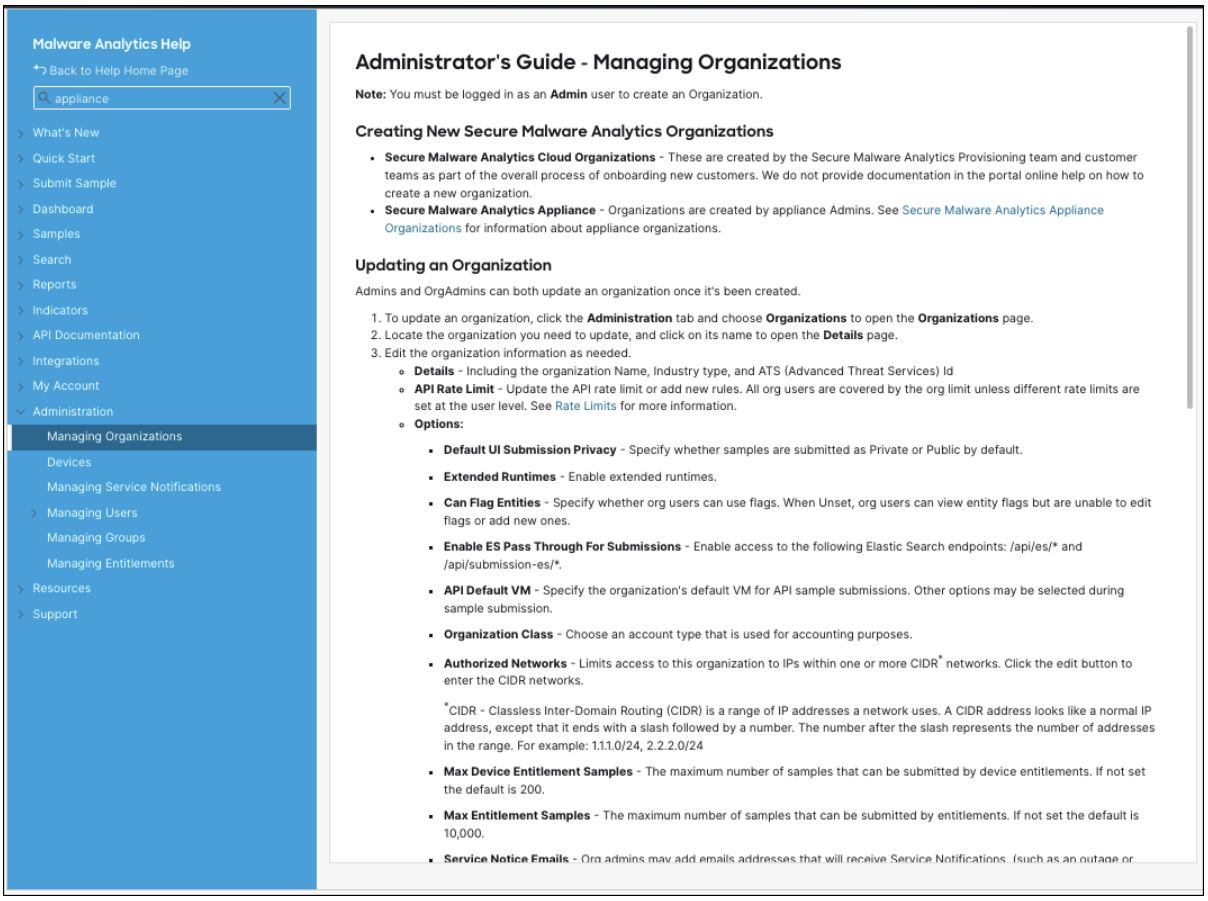
図 *3*: オンライン ヘルプ検索機能



Secure Malware Analytics Portal UI アドミニストレーション ガイド

管理者は、ポータルのオンライン ヘルプ トピックを参照できます。このトピックでは、ユーザーの管理方法やその他の情報を管理する方法について説明します。 **[アドミニストレーション]** タブをクリックし、 **アドミニストレーション ガイド]**を選択します。

図 *4 : Cisco Secure Malware Analytics* ポータル *UI* の管理ガイド



E メール セキュリティ アプライアンスと Web セキュリティアプライアンスに関する資料

E メール セキュリティ アプライアンス（ESA）または Web セキュリティアプライアンス（WSA）の接続に関する詳細については、「インバウンドおよびアウトバウンド接続」を参照してください。

ESA/WSA のオンラインヘルプまたはユーザーガイドの「Enabling and Configuring File Reputation and Analysis Services」の手順を参照してください。

- *Cisco Secure Email Gateway ユーザー ガイド*
- *Cisco Secure Web Appliance ユーザーガイド*

ログイン名とパスワード（デフォルト）

デフォルトのログイン名とパスワードを次の表に示します。

ユーザー（User）	ログイン/パスワード
Admin UI とシェルユーザー	最初のSecure Malware Analytics/Admin TUI でランダムに生成されたパスワードを使用し、次にAdmin UIの構成ワークフローの最初の手順で入力した新しいパスワードを使用します。 パスワードを紛失した場合は、「管理者パスワードのリセット」の手順に従ってください。
Cisco Secure Malware Analytics Web ポータル UI 管理者	ログイン：**admin** パスワード：最初のAdmin UIパスワードを使用して初期化します。初期化の後、独立した状態になります。
CIMC	Login: **admin** Password: **password**

パスワード条件

パスワードには、次が含まれている必要があります。

- 8文字以上
- 1つ以上の数字
- 1 つ以上の特殊文字
- 大文字および小文字

管理者パスワードのリセット

デフォルトの管理者パスワードは、アプライアンスの初期設定と設定の際にAdmin TUIでのみ表示されます。初期設定が完了すると、管理者パスワードは、読み取り可能なテキストで表示されなくなります。

（注） LDAP認証は、複数の管理者がいる場合に、Admin TUIとAdmin UIログインに使用できます。アプライアンスにLDAP認証のみが設定されている場合、リカバリ モードでパスワードをリセットすると、認証モードが再設定され、システムパスワードでもログインできるようになります。

管理者パスワードを紛失してAdmin UIにログインできない場合は、次の手順を実行してパスワードをリセットします。

手順

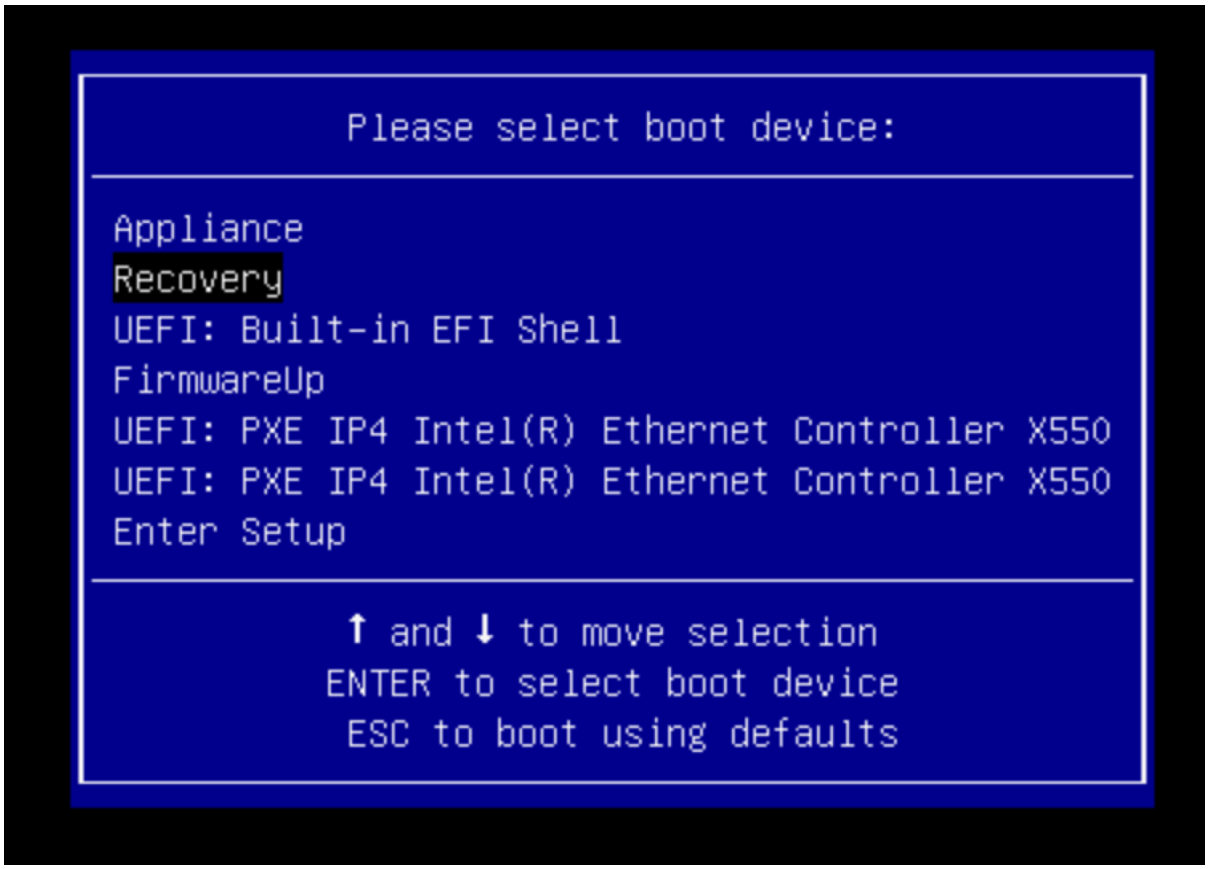
ステップ 1 Cisco Secure Malware Analytics アプライアンスを再起動します。 **[操作（Operations）**] タブをクリックして **[電源（Power）]**を選択し、[再 **起動（Reboot）]** ボタンをクリックします。アプライアンスが再起動し、[BIOS] ウィンドウが開きます。

図 *5 : [BIOS]* ウィンドウ - *[*ブートの選択（*Choose Boot*）*]* メニュー*<F6>*リカバリモード用

ステップ 2 [BIOS] ウィンドウで、 **F6** を押して **[Boot]** メニューを開きます。

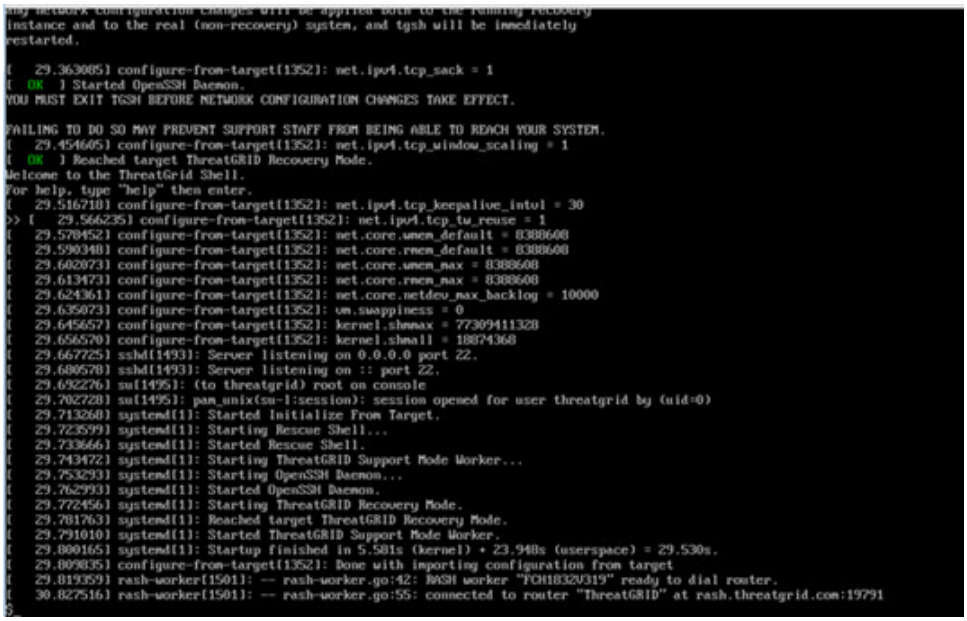
ステップ 3 **[リカバリ（Recovery）]** を選択し、 **[Enter]**を押します。

図 *6:* ブート メニュー



Cisco Secure Malware Analytics シェルがリカバリ モードで開きます。

図 *7:* リカバリ モードの *Cisco Secure Malware Analytics* シェル（*tgsh*）



ステップ 4 `passwd` を実行して、パスワードを変更します。

図 *8 : Enter New Password*

（注）
このモードではコマンドプロンプトが常に表示されるとは限りません。また、ロギング出力がいずれかの時点で入力と重なるように表示されることがあります。この表示は入力には影響しません。ブラインド入力を続けることができます。2 行のロギング出力は無視します。

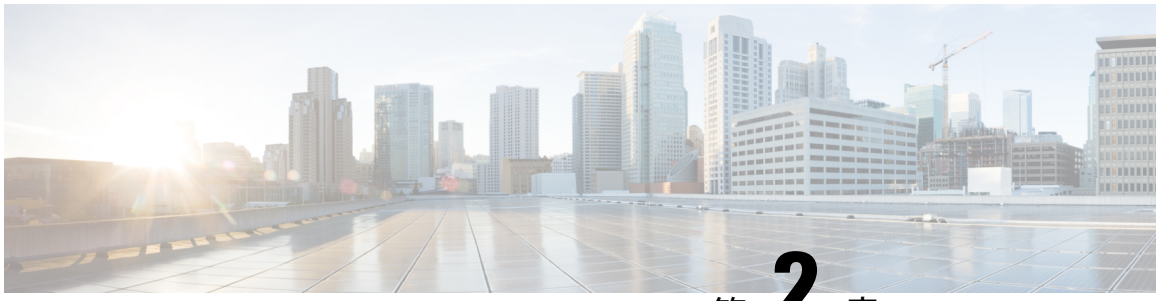
ステップ 5 パスワードを（ブラインドで）入力し、**Enter** キーを押します。

ステップ 6 パスワードをもう一度入力して、**Enter** キーを押します。

（注）
パスワードは表示されません。

ステップ 7 「**Reboot**」と入力し、**Enter** キーを押して、アプライアンスを通常モードで起動します。

（注）
パスワードのリセットを有効にするために再起動前に exit コマンドを実行する必要はなくなりました（v2.10 以降）。



第 2 章

計画

Cisco Secure Malware Analytics アプライアンスは、出荷前にシスコの製造部門によってインストールされた Cisco Secure Malware Analytics ソフトウェアを備える Linux サーバです。Cisco Secure Malware Analytics アプライアンスを受け入れた場合、オンプレミスのネットワーク環境用に設定および構成する必要があります。

この章では、設定と構成の前に確認する必要がある環境、ハードウェア、およびネットワークの要件について説明します。

サポートされるブラウザ

Cisco Secure Malware Analytics は、次のブラウザをサポートしています。

- Google Chrome™

- Mozilla Firefox®
- Apple Safari®

（注） Microsoft® Internet Explorer® はサポートされて**いません**。

環境要件

Cisco Secure Malware Analytics アプライアンス（v2.7.2 以降）は、Cisco Secure Malware Analytics M5 アプライアンスサーバーに展開されます。Cisco Secure Malware Analytics アプライアンスをセットアップして設定する前に、『*Cisco Threat Grid M5* ハードウェア設置ガイド』の仕様に従って、電源、ラックスペース、冷却、およびその他の問題に必要な環境要件を満たしていることを確認してください。

ハードウェア要件

管理インターフェイスには、SFP+ フォームファクタが使用されています。Cisco Secure Malware Analytics アプライアンスをクラスタリングしている場合は、それぞれの顧客インターフェイスで追加の SFP+ モジュールが必要になります。

（注） SFP+ モジュールは、設定ウィザードを実行するセッションでCisco Secure Malware Analytics アプライアンスの電源を入れる前に接続する必要があります。

スイッチで使用できる SFP+ ポートがない、または SFP+ が望ましくない場合は、1000Base-T のトランシーバ（シスコ機器互換のギガビット RJ 45 銅線 SFP トランシーバモジュール Mini -GBIC - 10/100/1000 Base-T 銅線 SFP モジュールなど）を使用できます。

図 *9 : Cisco 1000BASE-T* 銅線 *SFP*（*GLC-T*）

サーバーにモニターを接続できます。または、Cisco Integrated Management Controller（CIMC）が設定されている場合は、リモート KVMを使用できます（UCS C220-M3 および C220-M4 サーバー上で）。

（注） CIMC は、Cisco Secure Malware Analytics M5 アプライアンス サーバではサポートされていません。

CISCO UCS Power Calculator は、推定電力を算出するために使用できます。

ネットワーク要件

Cisco Secure Malware Analytics アプライアンスには、次の 3 つのネットワークが必要です。

- **ADMIN**：Cisco Secure Malware Analytics アプライアンスの設定を行うには、管理ネットワークを設定する必要があります。
  - Admin UI 管理トラフィック（HTTPS）
  - SSH
  - NFSv4（発信。IP ではなく NFS ホスト名が使用される場合、この名前がダーティ DNS 経由で解決されます）。
- **クリーン**：クリーンネットワークは、インバウンド、Cisco Secure Malware Analytics アプライアンスへの信頼済みトラフィック（要求）、および Cisco E メール セキュリティ アプライアンスや Web セキュリティアプライアンスなどの統合アプライアンスに使用されます。統合アプライアンスは、クリーン インターフェイスの IP アドレスに接続します。

（注） クリーン ネットワーク インターフェイスの URL は Admin UI の設定が完了するまで機能しません。

注：以下の制限付きタイプのネットワークトラフィックは、クリーンインターフェイスから発信することができます。

- リモート syslog 接続
- Cisco Secure Malware Analytics アプライアンスによって送信される電子メールメッセージ
- Cisco Secure Endpoint プライベート クラウド デバイスへの配置更新サービス接続
- DNS 要求（上記のいずれかに関連するもの)
- LDAP
- RADIUS トラフィック

- **ダーティ**：「ダーティ」ネットワークは Cisco Secure Malware Analytics Appliance アプライアンスからの発信トラフィック（マルウェア トラフィックを含む）に使用されます。

（注） 内部ネットワークアセットを保護するために、企業の IP とは異なる専用の外部 IP アドレス（ダーティインターフェイスなど）を使用することをお勧めします。

ネットワーク インターフェイスの設定については、「ネットワーク インターフェイス」を参照してください。

DNS サーバ アクセス

配置更新サービスのルックアップ、リモートの Syslog 接続の解決、および Secure Malware Analytics ソフトウェアからの通知に使用されるメールサーバーの解決以外の目的に使用される DNS サーバーは、ダーティネットワークを介したアクセスが可能になっている必要があります。

デフォルトでは、DNS はダーティ インターフェイスを使用します。クリーン インターフェイスは Secure Endpoint プライベート クラウドの統合およびその他のサービスに使用されます。Secure Endpoints プライベート クラウドのホスト名がダーティ インターフェイスに解決できない場合、クリーン インターフェイスを使用する別の DNS サーバーを Admin UI に構成できます。

NTP サーバ アクセス

デフォルトで、NTP サーバは、ダーティ ネットワークを介してアクセスできる必要があります。

2.12 リリース以降、アプライアンスは、ダーティインターフェイス（デフォルト）ではなく、クリーンインターフェイスから NTP サーバーに接続するように任意で構成できます。これにより、内部 NTP サーバを使用できるようになります。

統合

Secure Malware Analytics アプライアンスを他の Cisco 製品（E メール セキュリティ アプライアンス、Web セキュリティ アプライアンス、または Secure Endpoint プライベート クラウドなど）とともに使用する場合、追加の計画が必要になることがあります。詳細については、ESA または WSA の Secure Malware Analytics アプライアンスへの接続を参照してください。

DHCP 要件

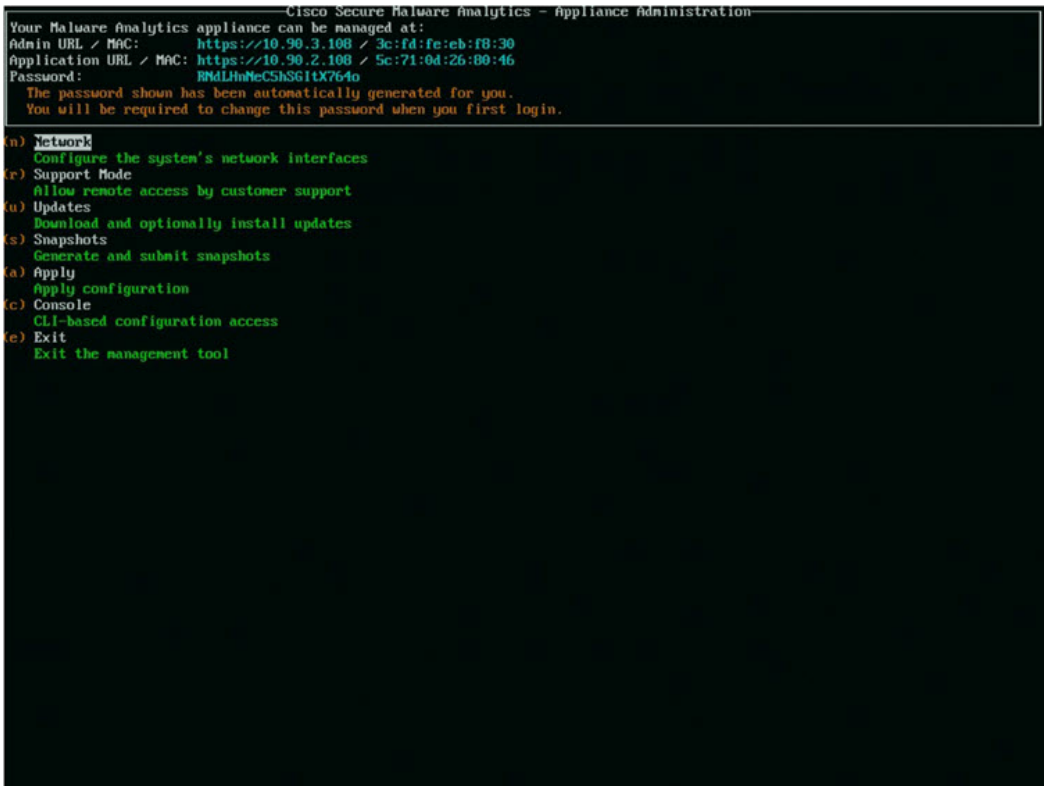
ただし、DHCPを使用するように設定されたネットワークに接続している場合は、要件を理解することが重要です。DHCP を使用する Cisco Secure Malware Analytics アプライアンスでは、DNS を明示的に指定する必要があります。

警告 DNS サーバーが明示的に指定されていないシステムのアップグレードは失敗します。

（注） Admin TUI には、Admin UI にアクセスして構成するために必要な情報が表示されます。アプライアンスの起動後、DHCPのIPアドレスが表示されるまでに時間がかかる場合があります。

Admin TUI（テキストモード UI）を開き、次の情報に注意してください。

図 *10 : Admin TUI*（*DHCP* を使用するためにネットワーク構成されて接続）



- [**Admin URL**]：管理ネットワーク。 Admin UI の残りの設定作業を継続するためにこのアドレスが必要です。
- [**Application URL**]：クリーンネットワーク。これは、 Admin UI で設定を完了した後に使用するアドレスです。

ダーティ ネットワークは表示されません。

- **[パスワード（Password）]**：Cisco Secure Malware Analytics アプライアンスのインストール時にランダムに生成される初期管理パスワード。後で、Admin UI 構成プロセスの最初の手順として、このパスワードを変更する必要があります。

最初の IP 割り当てを DHCP から静的 IP アドレスに変更する必要がある場合は、ネットワーク参照してください。

ライセンス

新しいアプライアンスを購入すると、ライセンスが生成され、**[構成（Configuration）] > [ライセンス（License）]**ページの**[サーバーからライセンスを取得（Retrieve License From Server）]**ボタンが有効になります。ただし、これが機能しない場合、または特別なケース（ライセンスがカスタム ワンオフであるなど）がある場合、ライセンスはパスワードを含む暗号化ファイルとして直接渡されます。

ライセンスに関して不明な点がある場合は、サポート ケースを開くにお問い合わせください。

レート制限

API サンプル送信レート制限は、ライセンス契約条件に基づいて Cisco Secure Malware Analytics アプライアンス全体に適用されます。API レート制限は API 送信にのみ適用され、手動によるサンプル送信には適用されません。

レート制限はカレンダー日ではなくローリング タイムの時間枠に基づきます。送信制限に達すると、次の API 送信の再試行まで待機する時間を通知するメッセージとともに、429 エラーが返されます。詳細については、ポータルのオンライン ヘルプを参照してください。

組織およびユーザー

Cisco Secure Malware Analytics アプライアンスの設定とネットワーク設定を完了したら、Cisco Secure Malware Analytics の初期組織を作成してユーザー アカウントを追加する必要があります。これにより、ユーザーはログインして、分析用にマルウェア サンプルの送信を開始できるようになります。このタスクでは、要件に応じて、複数の組織およびユーザ間のプランニングや調整が必要になることがあります。

詳細については、新規組織の作成および「Cisco Secure Malware Analytics ポータルヘルプ」（**[管理（Administration）] > [管理者ガイド（Administrator's Guide）]** をクリックして管理ガイドのトピックを開きます）を参照してください。

更新

更新プログラムをインストールする前に、初期 Cisco Secure Malware Analytics アプライアンスのセットアップと設定手順を**完了する必要があります**。このガイドに記載されている初期構成の完了後、すぐに更新を確認することをお勧めします（『*Cisco Threat Grid Appliance Getting Started Guide*』を参照）。

Cisco Secure Malware Analytics アプライアンスのセットアップと設定手順 アプライアンスの更新は、ライセンスがインストールされ、カスタマー サポートにより別段指示される場合を除き、ダウンロードできません。また、更新プロセスでは、最初のアプライアンスの設定が完了している必要があります。更新は、順に実行する必要があります。

ユーザー インターフェイス

サーバをネットワークに接続し、正常に起動した後で Secure Malware Analytics アプライアンスを構成するために、複数のユーザ インターフェイスを利用できます。

（注） LDAP 認証は、管理 TUI および管理 UI で使用できます。RADIUS 認証は、Secure Malware Analytics アプリケーション UI（バージョン 2.10 以降）で使用できます。

管理 TUI

Admin TUI インターフェイスは、 ネットワーク インターフェイスを設定するために使用されます。Cisco Secure Malware Analytics アプライアンスが正常に起動すると、Admin TUI が表示されます。

Admin TUI への再接続

Admin TUI はコンソール上で開いたままになり、アプライアンスにモニターを接続するか、（CIMC が設定されている場合は）リモート KVM を使用することでアクセスできます。

（注） CIMC は、Cisco Secure Malware Analytics M5 アプライアンス サーバではサポートされていません。

Admin TUI に再接続するには、ユーザー「**threatgrid**」として管理 IP アドレスに SSH 接続します。

必要なパスワードは、ランダムに生成される初期パスワードであり、最初に Admin TUI に表示されたパスワードか、OpAdmin 設定の最初の手順で作成した新しい管理者パスワードです（『*Cisco Threat Grid Appliance Getting Started Guide*』を参照してください）。

Threat Grid シェル（tgsh）

Threat Grid シェル（tgsh）は、コマンド（estroy-data や forced backup など）を実行するために使用される管理者のインターフェイスであり、専門家による低レベルのデバッグにも使用されます。tgsh にアクセスするには、管理 TUI で **[コンソール（CONSOLE）]** を選択します。

（注） Admin UI は Cisco Secure Malware Analytics ユーザーと同じログイン情報を使用するため、tgsh を介して行われたパスワードの変更や更新は Admin UI にも影響します。

注意 tgsh によるネットワーク設定の変更は、Cisco Secure Malware Analytics サポートによって特に指示された場合を除き、サポートされません。代わりに Admin UI または Admin TUI ダイアログを使用する必要があります。2.12 リリースでは、管理者の電子メール、Grovebox URL、SMTP 設定などを変更するオプションが削除されました。アプライアンスのワイプ操作が、ブートローダメニューではなく、リカバリモード tgsh 内でアクティブ化されるようになりました。

Admin UI

Admin UI は、Cisco Secure Malware Analytics アプライアンスの管理者の主な構成インターフェイスです。Cisco Secure Malware Analytics アプライアンスの管理インターフェイスで IP アドレスが設定された後に使用できる Web ポータルです。

ライセンス、電子メールホスト、SSL 証明書など、Cisco Secure Malware Analytics アプライアンス設定の多くは Admin UI からのみ実行できます。

（注） 初期設定および構成ウィザードについては、『Cisco Secure Malware Analytics アプライアンスの設定およびコンフィギュレーション ガイド』を参照してください。

Admin UI のコンポーネント

次のセクションでは、Admin UI を使用して設定するために必要な詳細について説明します。

- ホーム （57 ページ）
- 構成
- ステータス
- 操作
- サポート

Cisco Secure Malware Analytics ポータル

Cisco Secure Malware Analytics のユーザー インターフェイス アプリケーションは、クラウド サービスとして利用でき、Cisco Secure Malware Analytics アプライアンスにもインストールされています。Cisco Secure Malware Analytics クラウドサービスと、Cisco Secure Malware Analytics アプライアンスに含まれる Cisco Secure Malware Analytics ポータルの間に通信はありません。

ネットワーク インターフェイス

使用可能なネットワーク インターフェイスを次の表に示します。

インターフェイス	説明
Admin	• 管理ネットワークに接続します。管理ネットワークからの**着信のみ**。 • Admin UI トラフィック • Admin TUI 用の SSH（インバウンド） • バックアップとクラスタリング用の NFSv4（発信）IP ではなく NFS ホスト名が使用される場合、この名前がダーティ DNS 経由で解決されます）。すべてのクラスタ ノードからアクセスできる必要があります。 • Admin ポートは（tgsh シェルから）v2.11 で Admin UI から無効にすることができます。無効になっている場合、クラスタ化されていない Cisco Secure Malware Analytics アプライアンスは、クリーン ポートとダーティー ポートが接続されている場合のみ正しく動作します。管理 UI はクリーン インターフェイスのポート 8443（v2.11 リリースではポート 18443 も）に表示されます。ポートが無効になっていない場合、管理ポートを切断すると、Cisco Secure Malware Analytics アプライアンスの一部しか機能しなくなります（または、最高でも部分的にしか機能しません）。 **（注）** 管理インターフェイス用のフォーム ファクタは SFP+ です。「ハードウェア要件」を参照してください。
クラスタ	管理用ではない SFP+ ポートはクラスタリングに使用されます。 • クラスタリングに必要なクラスタ インターフェイス（任意） • ダイレクト インターコネクトには追加の SFP+ モジュールが必要です。このインターフェイスでは、設定の必要はありません。アドレスが自動的に割り当てられます。

インターフェイス	説明
[クリーン（Clean）]	• クリーンネットワークに接続します。クリーンには、社内ネットワークからアクセスできる必要がありますが、インターネットへの発信アクセスができないようにする必要があります。 • UI および API トラフィック（着信） • サンプルの送信 • SMTP（設定済みメール サーバーへの発信接続） • SSH（Admin TUI 用のインバウンド） • syslog（設定済み syslog サーバーへの発信） • ESA/WSA と CSA の統合 • Secure Endpoint プライベート クラウド統合 • DNS（オプション） • LDAP（発信） • RADIUS（発信） • [NTP]（内部 NTP サーバーを使用する場合）

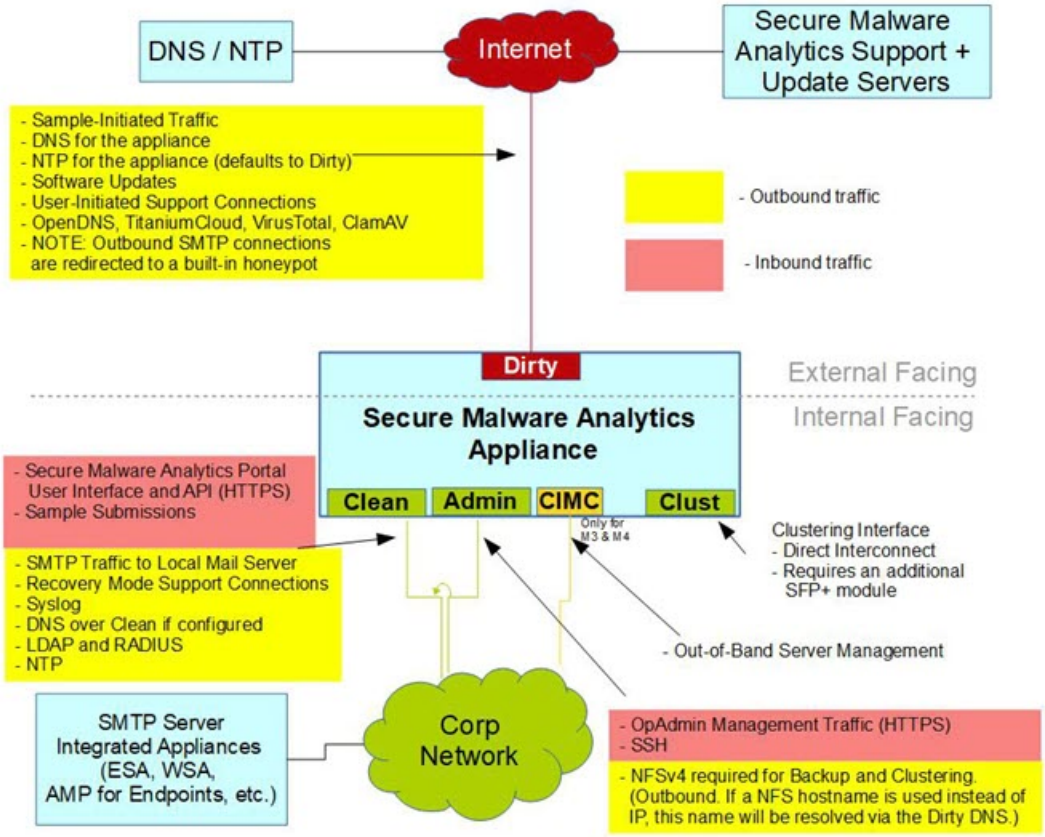
インターフェイス	説明
ダーティ	ダーティネットワークに接続します。インターネットアクセスが必要です。発信のみ。 プライベート IP に送信されるトラフィックは、ネットワーク出口のローカリゼーション ファイアウォールでドロップされるため、ダーティインターフェイスには独自の DNS（プライベート IP）を使用しないようにしてください。 • DNS （注） Cisco Secure Endpoint プライベートクラウドとの統合を設定し、Cisco Secure Endpoints アプライアンスのホスト名がダーティインターフェイスで解決できない場合、クリーンインターフェイスを使用する別の DNS サーバーを Admin UI に設定できます。 • NTP（デフォルトは Dirty） • 更新 • サポート セッション • サポートスナップショット • マルウェアサンプルから開始されたトラフィック • OpenDNS, TitaniumCloud, VirusTotal, ClamAV_signature updates • SMTP の発信接続が組み込みのハニーポットにリダイレクト （注） ダーティインターフェイスでの IPv4LL アドレス空間（168.254.0.16）の使用はサポートされていません。
CIMC インターフェイス	Cisco Integrated Management Controller（CIMC）インターフェイスが設定されている場合は、サーバーの管理とメンテナンスに使用できます。「CIMC の設定」を参照してください。 （注） CIMC は、Cisco Secure Malware Analytics M5 アプライアンス サーバではサポートされていません。

ネットワーク インターフェイスの設定図

このセクションでは、Cisco Secure Malware Analytics アプライアンスの最も論理的で推奨される設定について説明します。ただし、お客様によってインターフェイス設定は異なります。

ネットワーク要件に従って、ダーティインターフェイスを内部に接続する場合や、クリーンインターフェイスを適切なネットワークセキュリティ対策が施されている外部に接続する場合があります。

図 *11* : ネットワーク インターフェイスの設定図



（注） Cisco Secure Malware Analytics アプライアンス（v 2.7.2 以降）では、 **enable_clean_interface** オプションは使用できますが、デフォルトでは無効になっています。このオプション（設定を適用して再起動した後）は、割り当てられたクリーン IP のポート 8443 および 18443 の管理インターフェイスへのアクセスを有効にします。管理イーサネットインターフェイスを無効にすると、クリーンのポート 8843 でのこのアクセスも有効になります。

ファイアウォール ルール

ここでは、推奨されるファイアウォールルールについて説明します。

（注） ポート 22 および 19791 のダーティインターフェイス上で制限付きの発信ポリシーを実装すると、経時的な更新の追跡が必要となり、ファイアウォールの維持等により多くの時間がかかる可能性があります。

（注） ダーティインターフェイスでの IPv4LL アドレス空間（168.254.0.16）の使用はサポートされていません。

ダーティ インターフェイスによる発信

送信元	送信先	プロトコル	ポート	操作	コメント
ダーティインターフェイス	インターネット	ANY	ANY	許可（Allow）	サンプルからのアウトバウンドトラフィックを許可します。オプションで、Cisco のデータセンターを介してプロキシされます。（正確な結果を取得するには、指定されたポートやプロトコルにかかわらず、マルウェアからコマンド アンド コントロール サーバーへのアクセスが許可されている必要があります。）

ダーティ インターフェイスによる着信

送信元	送信先	プロトコル	ポート	操作	コメント
ANY	ダーティインターネット	ANY	ANY	拒否（Deny）	すべての着信接続を拒否します。

クリーン インターフェイスによる発信

送信元	送信先	プロトコル	ポート	操作	コメント
クリーンインターフェイス	SMTP サーバー	TCP	25	許可（Allow）	アプライアンスはクリーン インターフェイスを使用して、設定済みメールサーバーへの SMTP 接続を開始します

クリーンインターフェイスによる発信（任意）

送信元	送信先	プロトコル	ポート	操作	コメント
クリーンインターフェイス	企業の DNS サーバー	TCP/UDP	53	許可（Allow）	任意。クリーン DNS が構成されている場合のみ必須
クリーンインターフェイス	AMP プライベート クラウド	TCP	443	許可（Allow）	任意。Cisco Secure Endpoint プライベート クラウド統合が使用されている場合のみ必須。
クリーンインターフェイス	Syslog サーバー	UDP	514	許可（Allow）	Syslog メッセージおよび Cisco Secure Malware Analytics 通知を受信するように指定されたサーバへの接続を許可
クリーンインターフェイス	LDAP サーバー	TCP/UDP	389	許可（Allow）	任意。LDAP が構成されている場合のみ必須
クリーンインターフェイス	LDAP サーバー	TCP	636	許可（Allow）	任意。LDAP が構成されている場合のみ必須
クリーンインターフェイス	RADIUS サーバー	DTLS	2083	許可	Cisco Secure Malware Analytics アプリケーション UI（Face）へのログインを許可します。任意。RADIUS が設定されている場合のみ必須。
クリーンインターフェイス	インターネット	UDP	123	許可（Allow）	オプションで、このオフバイ デフォルト機能を使用して、内部 NTP サーバーを使用できます。

クリーン インターフェイスによる着信

送信元	送信先	プロトコル	ポート	操作	コメント
ユーザー サブネット	クリーン インターフェイス	TCP	22	許可（Allow）	Admin TUI への SSH 接続を許可します。

送信元	送信先	プロトコル	ポート	操作	コメント
ユーザーサブネット	クリーン インターフェイス	TCP	80	許可（Allow）	アプライアンス API と Cisco Secure Malware Analytics のユーザーインターフェイス。これは HTTPS TCP/443 にリダイレクトします。
ユーザーサブネット	クリーン インターフェイス	TCP	443	許可（Allow）	アプライアンス API と Cisco Secure Malware Analytics のユーザーインターフェイス。
ユーザーサブネット	クリーン インターフェイス	TCP	9443	許可	Cisco Secure Malware Analytics UI Glabbox への接続を許可します。

管理インターフェイスによる発信（任意）

以下は、設定されるサービスの内容に依存します。

送信元	送信先	プロトコル	ポート	操作	コメント
管理インターフェイス	NFSv4 サーバー	TCP	2049	許可（Allow）	任意。Secure Malware Analytics アプライアンスが NFSv4 共有にバックアップを送信するように設定されている場合のみ必須。

管理インターフェイスによる着信

送信元	送信先	プロトコル	ポート	操作	コメント
管理サブネット	管理インターフェイス	TCP	22	許可（Allow）	Admin TUI への SSH 接続を許可します。
管理サブネット	管理インターフェイス	TCP	80	許可（Allow）	Admin UI へのアクセスを許可します。これは HTTPS TCP/443 にリダイレクトします。
管理サブネット	管理インターフェイス	TCP	443	許可（Allow）	Admin UI へのアクセスを許可します。

シスコ未検証/導入が推奨されるダーティ インターフェイス

Cisco 以外の検証済み/推奨 ：ファイアウォール アウトバウンド トラフィックは、マルウェアがコマンドアンドコントロールインフラストラクチャに接続するのを防ぎ、そのコマンドアンドコントロール インフラストラクチャからダウンロードされるものを決定する試みを制限することで有効性を低下させる可能性があります。

送信元	送信先	プロトコル	ポート	操作	コメント
ダーティインターフェイス	インターネット	TCP	22	許可（Allow）	更新、サポートスナップショット、ライセンスのサービス。
ダーティインターフェイス	インターネット	TCP/UDP	53	許可（Allow）	発信 DNS を許可。
ダーティインターフェイス	インターネット	UDP	123	許可（Allow）	発信 NTP を許可します。
ダーティインターフェイス	インターネット	TCP	19791	許可（Allow）	Cisco Secure Malware Analytics サポートへの節ゾックを許可します。
ダーティインターフェイス	Cisco Umbrella	TCP	443	許可（Allow）	サードパーティの検出およびエンリッチメントサービスと結合します。
ダーティインターフェイス	VirusTotal	TCP	443	許可（Allow）	サードパーティの検出およびエンリッチメントサービスと結合します。
ダーティインターフェイス	TitaniumCloud	TCP	443	許可（Allow）	サードパーティの検出およびエンリッチメントサービスと結合します。

プライバシーとサンプルの可視性

分析のため Cisco Secure Malware Analytics アプライアンスにサンプルを送信する際、コンテンツのプライバシーが重要な考慮事項となります。機密文書やアーカイブタイプの資料が分析用に送信される場合、プライバシーは特に重要な考慮事項になります。機密情報を見つけることは、特に検索 API を使用して Cisco Secure Malware Analytics アプライアンスにアクセスできるユーザーにとって、比較的簡単である可能性があるためです。

Cisco Secure Malware Analytics へのサンプル送信に関するプライバシーとサンプルの可視性モデルは次のとおりです。

- サンプルは、プライベートに指定されていない限り、送信者の組織外のユーザーに表示されます。
- プライベートサンプルは、サンプルを送信したユーザーと同じ組織内の Cisco Secure Malware Analytics ユーザーのみが閲覧できます。

統合により送信されたサンプル

統合から送信されたサンプルの場合、 Cisco Secure Malware Analytics アプライアンスでのプライバシーおよびサンプルの可視性モデルは変更されます。統合とは、E メール セキュリティ アプライアンス（ESA）、Web セキュリティアプライアンス（WSA）および他のデバイスなどのシスコ製品や、サードパーティのサービスのことです（CSA 統合という用語は、Cisco Sandbox API 経由で Cisco Secure Malware Analytics アプライアンスに統合（または登録）されている、ESA/WSA その他の Cisco 製アプライアンス、デバイス、サービスを意味します）。

Cisco Secure Malware Analytics アプライアンスでのすべてのサンプル送信は、デフォルトでパブリックに設定されるため、所属する組織にかかわりなく、統合を含む他のすべてのアプライアンスユーザーが表示できます。アプライアンスのすべてのユーザが、他のすべてのユーザが送信したサンプルのあらゆる詳細を確認できるということです。

Cisco Secure Malware Analytics のユーザーはまた、プライベートなサンプルも Cisco Secure Malware Analytics アプライアンスに送信します。それは統合に含まれ、サンプルの送信者と同じ組織からの他の Cisco Secure Malware Analytics アプライアンス ユーザーにのみ表示されます。

次の表で、Cisco Secure Malware Analytics アプライアンスでのプライバシーおよびサンプルの可視性モデルについて説明します。

図 *12 : Cisco Secure Malware Analytics* アプライアンスでのプライバシーと可視性

Sample and Analysis Results are visible to:	Public Submissions (Default)	Private Submissions	CSA Integration Submissions (Public by Default)
Users from the Same Organization	✔	✔	✔
Users from a Different Organization	✔	✔	✔
CSA Integrations from the Same Organization	✔	✔	✔
CSA Integrations from a Different Organization	✔	✖	✔

- **フルアクセス**：緑色のチェックマークは、ユーザーがサンプルと分析結果にフルアクセスできることを示します。
- **スクラビングレポート**：灰色のチェックマークは、プライベート送信の結果がスクラビングされたことを示します。ユーザーはサンプルと分析結果への部分的なアクセス権を持っていますが、サンプルに関する潜在的な機密情報はすべて削除されます。Glovebox には、ファイル名、プロセス名、スクリーンショット、またはアクティビティについての詳細情報は表示されません。

  サンプルの送信者のログイン情報などの詳細情報を [Metadata] セクションから除外します。ビジネスの過程でプライベートサンプルからハッシュが発生した場合、既知の脅威に対する警告が表示されます。さらに詳細な情報が必要な場合は、完全な分析のためにサンプルの独自のコピーを送信します。

  プライベートサンプルはダウンロードされない場合があります。スクラビングレポートには、アーティファクト（ファイル名が削除されたもの）、動作インジケータ、ドメイン、IP が含まれます。
- **アクセスなし**：赤色のXは、ユーザーがサンプルまたは分析結果にアクセスできないことを示します。

同じ基本的なプライバシー ルールが Cisco Secure Endpoint プライベート クラウドと Cisco Secure Malware Analytics アプライアンスの統合に適用されます。

アプライアンスのワイプ動作

Wipe アプライアンスの動作を使用すると、Cisco Secure Malware Analytics アプライアンスのディスクをワイプして、廃棄前にすべてのデータを削除したり、Cisco Demo Loan Program に戻したりすることができます。

重要 アプライアンスのワイプ手順を実行すると、Cisco Secure Malware Analytics アプライアンスは、再イメージ化のためにシスコに返却せずに動作しなくなります（但し、デモ ローン プログラムのお客様を除き、事前の合意がない場合、再イメージ化サービスを利用できることは保証されません）。

詳細については、アプライアンスのワイプ操作によるすべてのデータの削除参照してください。

お客様のデータ

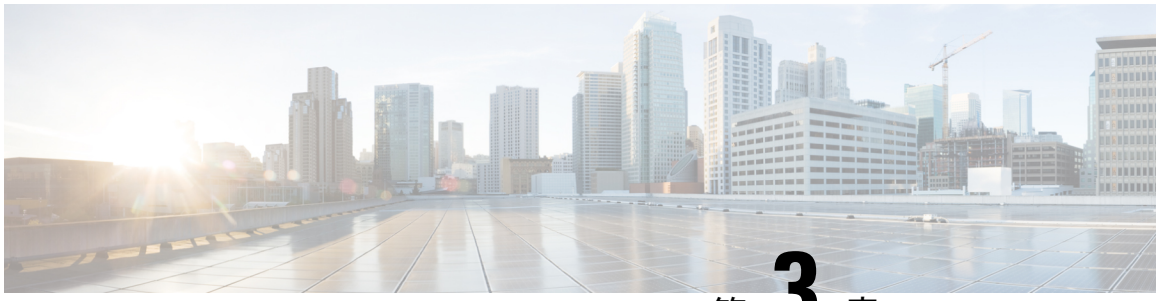
ログ、アクティブな設定、およびその他のお客様所有データは、データと OS ドライブに分散されるのではなく、ほぼ排他的にRAID 5データアレイに保存されます。OS ドライブに保存される残りのアプライアンス固有のコンテンツは、データドライブがマウントできない場合にリ

カバリモードを正しく動作させるために必要な情報に限定され、開示してもプライバシーへの影響は限定されます。

2.12 リリースでは OS アレイに保存されるコンテンツが少ないため、初期のアプライアンス（より小さい OS ドライブを搭載）では、データリセット中に必須のデフォルトイメージ以外の VM イメージを削除する（したがって、削除された VM イメージが再び利用可能になります）。

第 I 部

管理 TUI



第 3 章

ネットワーク

最初の Cisco Secure Malware Analytics アプライアンスネットワーク設定は、『*Cisco Threat Grid Appliance Getting Started Guide*』に記載されているように、管理 UI を使用してアプライアンスのセットアップ時に完了します。この章では、Admin TUI を使用して最初のネットワーク構成を変更する方法についての追加情報を提供します。

ネットワーク構成の変更

初期ネットワーク構成は、Admin TUI を使用して完了します。ネットワークの初期設定を変更する場合は、次の手順を実行します。

（注） DHCP を使用して IP を取得する場合は、「ネットワーク」を参照してください。

手順

ステップ 1 [Admin TUI] にログインします。

（注）
LDAP のみ（LDAP only） 認証に対して構成する場合、LDAP を使用して、Admin TUI にのみログインします。認証モードが **[LDAP またはシステム パスワード（LDAP or System Password）]** に設定されている場合、Admin TUI のログインで許可されるのは**システム** ログインのみです。

ステップ 2 管理 TUI インターフェイスで、 **[CONFIG_NETWORK]**を選択します。

[**Network Configuration**] コンソールが開き、現在のネットワーク設定が表示されます。

ステップ 3 必要な変更を行います（新しいエントリを入力する前に、バックスペースを押して古いエントリを削除する必要があります）。

ステップ 4 ダーティ ネットワークの [DNS Name] を空白のままにします。

ステップ 5 ネットワーク設定の更新が完了したら、Tab キーで下に移動し、**[検証（Validate）]** を選択してエントリを確認します。

エラーが発生する場合、無効な値を修正し、**[検証（Validate）]**をもう一度選択します。

検証が完了すると、[**Network Configuration**] ページに入力した値が表示されます。

ステップ 6 **[適用（Apply）]** を選択して構成設定を適用します。

行われた設定変更に関する詳細情報が表示されます。

ステップ 7 **[OK]** を選択します。

[**Network Configuration**] コンソールが再更新され、IP アドレスが表示されます。これで、ネットワークの設定は完了しました。

Admin TUI への再接続

Admin TUI はコンソール上で開いたままになり、アプライアンスにモニターを接続するか、（CIMC が設定されている場合は）リモート KVM を使用することでアクセスできます。

Admin TUI に再接続するには、ユーザー「**threatgrid**」として管理 IP アドレスに SSH 接続します。必要なパスワードは、Admin TUI ダイアログに最初に表示される、ランダムに生成された初期設定パスワード、または Admin UI 構成の最初の手順で作成した新しい管理者パスワードのどちらかです。詳細については、 コンフィギュレーション ガイドの最新の『Cisco Secure Malware Analytics アプライアンス スタート ガイド』を参照してください。

リカバリ モードでのネットワークの構成

リカバリモードでのネットワークの設定は、システム全体に反映されます（バージョン2.7 以降）。

- すべてのインターフェイスが起動します。
- ファイアウォールルールとポリシールーティングにより、どのプロセスがどのインターフェイスで通信するかが制限されます。

（注） ポート 19791 のサポートモードトラフィックは、3 つのインターフェイスすべての許可リストに含まれています。

リカバリモードでネットワーキングを設定するには、次の手順を実行します。

手順

ステップ 1 Cisco Secure Malware Analytics アプライアンスを再起動し（**[操作（Operations）] > [電源（Power）] > [再起動（Reboot）]**）、ブート メニューで **[リカバリモード（Recovery Mode）]** を選択します。

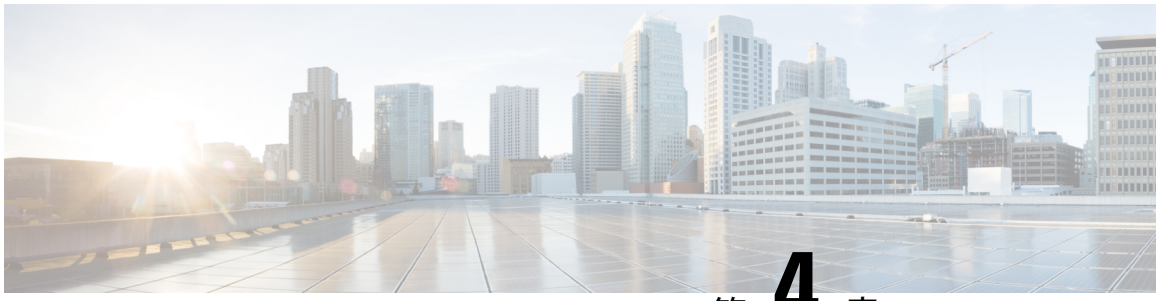
ステップ 2 システムが起動したら、**Enter** キーを数回押して clean コマンド プロンプトを表示させます。

ステップ 3 「**netctl clean**」と入力し、次の情報を入力します。

- **構成タイプ (dhcp|static)[Current: DHCP]**: static
- **IPアドレス(ipaddr)** : <Clean IP Address>
- **ネットマスク（ipaddr）** : <Netmask>
- [**Gateway Address**] : <クリーン ネットワーク ゲートウェイ>
- **[このインターフェイスのアドレスの DNS 名**（DNS name of this interface's address）]：このインターフェイスのアドレスの DNS 名を入力します。
- **[LAN アドレス用のプライマリ DNS サーバー**（Primary DNS server for LAN addresses）]：プライマリ DNS サーバー アドレスを入力します。
- **[LAN アドレス用のセカンダリ DNS サーバー（Secondary DNS server for LAN addresses）]**：セカンダリ DNS サーバー アドレスを入力します。
- **このプロファイルを保存しますか？(Yes|No)** : **はい（Yes**）と入力します

ステップ 4 構成を適用するために、**netconfig-apply** を入力します。

アプライアンスは、ポート 19791/tcp のクリーンインターフェイスでアウトバウンドサポート接続を開こうとします。



第 4 章

サポート対象のモード

Cisco Secure Malware Analytics（Threat Grid）アプライアンスのサポートモードは、認定された Cisco サポートスタッフがリモートアクセスしてアプライアンスを直接検査し、問題を診断およびトラブルシューティングできるようにする機能です。これは、ログ分析やサポートスナップショットなどの従来の方法だけでは解決できない複雑な問題のトラブルシューティングに役立ちます。

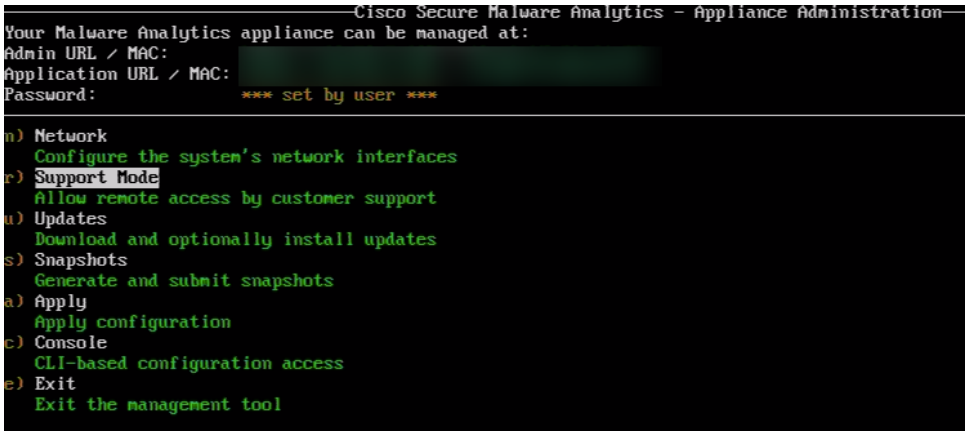
（注） Admin UI で同じ操作を実行することもできます。詳細については、「ライブ サポート セッション （147 ページ）」を参照してください。

ライブ サポート セッションの有効化

手順

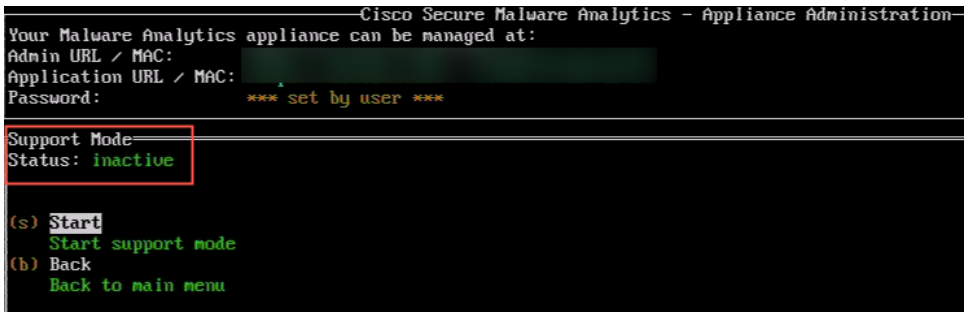
ステップ 1 **開始**： アプライアンスの所有者であるユーザーが、Cisco サポートとのライブ サポート セッションを開始します。これは、アプライアンスの Web インターフェイスまたはコマンドラインから実行できます。

図 *13 :* サポート対象のモード



ステップ 2 **サポート モードの有効化**：セッション中に、サポート担当者がサポートモードの有効化を要求する場合があります（STARTオプションを切り替えます）。[開始（Start）] を選択して、ライブ セッションを有効にします。ステータスが 非アクティブ から アクティブ に変更されたことを確認する必要があります。

図 *14 : [*開始（***Start***）*]* を選択して、ライブセッションを有効にします。



ステップ 3 **リモート アクセス**：有効にすると、Cisco のサポート スタッフは、安全なプロトコルを使用して「rash」コンポーネントにリモート ログインできます。これにより、次のようなアプライアンスのさまざまな側面を検査するための一時的なアクセスが付与されます。

- システム ログと構成ファイル
- 実行中のプロセスとリソース使用率
- 内部ネットワーク接続とトラフィック
- マルウェア分析の詳細と結果

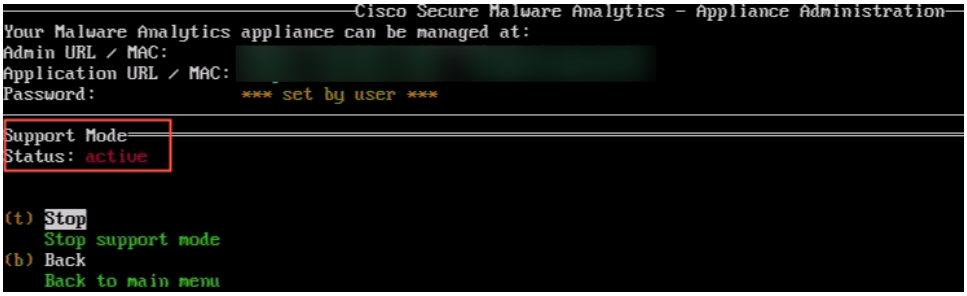
ステップ 4 **トラブルシューティングと解決策**：サポート スタッフは、アプライアンスを直接調べることで、問題をより深く理解し、次のようなアクションを実行できます。

- サービスの再開
- 構成の変更
- 特定の診断データの収集

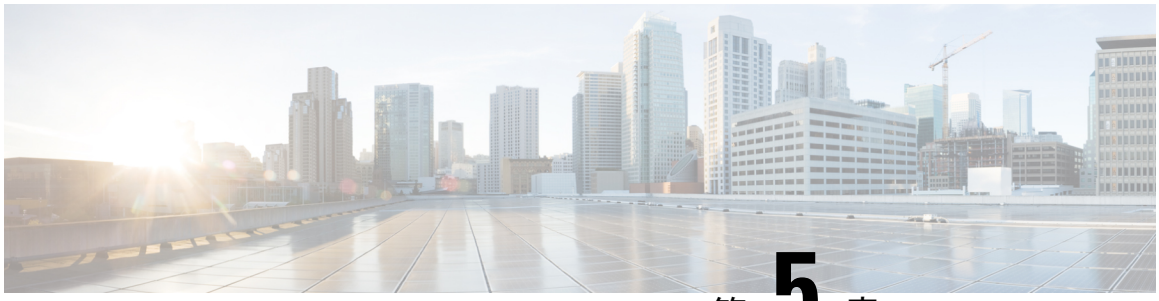
- 問題の根本原因を特定して解決

ステップ 5 **セッションの終了**：問題が解決するか、トラブルシューティングが完了したら、ライブ サポート セッションを終了することができます。これにより、サポート モードが自動的に無効になります。

図 *15 : [*停止（*Stop***）*]* を選択して、ライブ セッションを無効化します。**



[Status] がアクティブ から 非アクティブに切り替わります。



第 5 章

更新

[更新（Updates）] では、更新サーバ上のアプライアンスの更新を確認できます。

- アプライアンスの更新 （43 ページ）

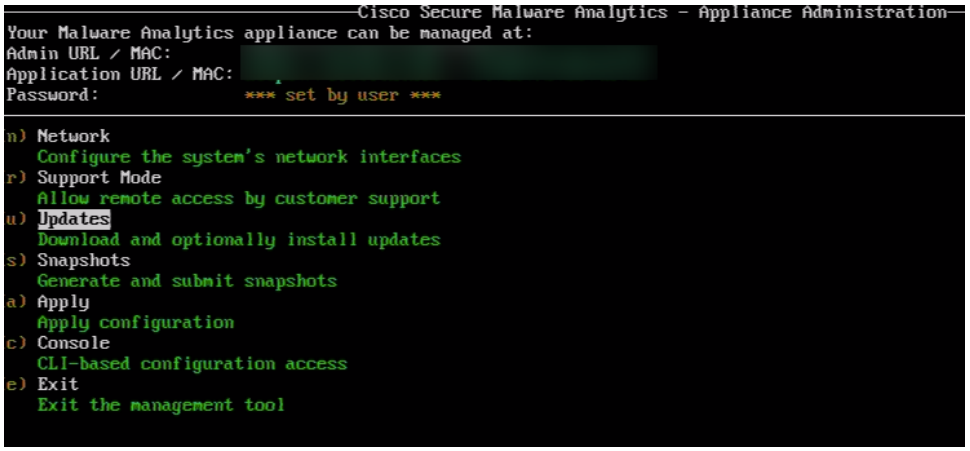
アプライアンスの更新

[更新（Updates）] では、アプライアンスの更新を確認、確認、ダウンロード、およびインストールできます。

手順

ステップ 1 [更新（Updates）] をクリックします。

図 *16 :* 更新

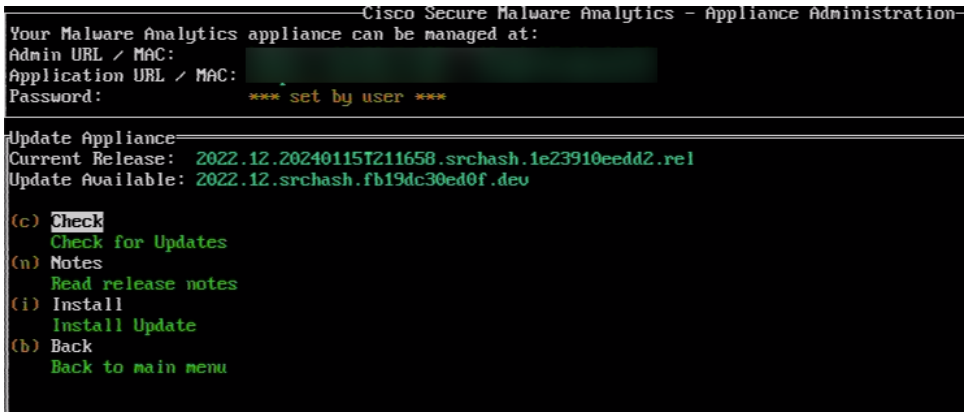


ステップ 2 以下をチェックする。

- 更新サーバで選択可能な更新をチェックするには、このオプションを選択します。
- 使用可能な更新のリストが、バージョン番号、リリース日、簡単な説明などで表示されます。

- 個別の更新を選択することも、ダウンロードするすべての更新を選択することもできます。

図 *17*:オプションの選択



ステップ 3 注：

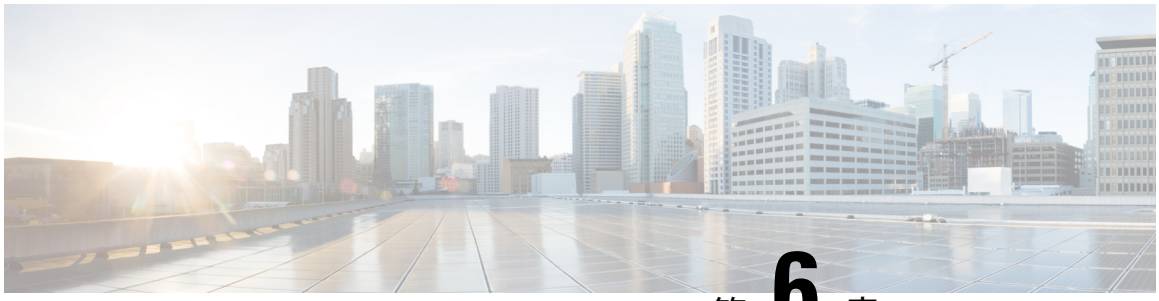
- 特定の更新のリリース ノートを参照するには、このオプションを選択します。
- リリースノートでは通常、新機能、バグ修正、セキュリティの改善、および更新に関連する既知の問題について詳しく説明しています。
- メモを確認することで、更新プログラムのインストールの潜在的な影響を理解することができます。

ステップ 4 インストール：

- 選択した更新をインストールするには、このオプションを選択します。
- インストールプロセスが指示されます。インストールプロセスには、選択内容の確認とライセンス契約の承認が含まれる場合があります。
- インストール時にシステムの再起動が必要になる場合があることに注意してください。それに応じて計画を立ててください。

ステップ 5 **Back**：

- 更新メニューを終了してメイン メニューに戻るには、このオプションを選択します。



第 6 章

スナップショット

スナップショットは、特定の時点での Cisco アプライアンスの重要な内部状態のキャプチャです。アプライアンスの設定、ログ、ネットワーク ステータス、およびその他の関連データを含む、アプライアンスの仮想画像のように機能します。

スナップショットが重要な理由

- **詳細な診断**：問題の根本原因を特定するためにカスタマーサポートで分析可能な豊富な情報を提供します。このデータには次のものが含まれます。
  - システム ログ：イベント、エラー、設定変更を記録します。
  - ネットワーク ステータス：アクティブな接続、トラフィック フロー、およびネットワーク関連の問題を表示します。
  - バージョン履歴：関連する可能性がある最近のソフトウェアまたはファームウェアの更新を強調表示します。
  - システム状態：スナップショットの時点でアクティブな設定、プロセス、およびリソースをキャプチャします。
- **時間の節約**：スナップショットの分析は、多くの場合、アプライアンスにリモートでログインして情報を手動で収集するよりも時間がかかります。これは問題を迅速に解決できることを意味します。
- **再現性**：問題が再発した場合、カスタマーサポートはスナップショットにより、正確なアプライアンスの状態を再作成して詳細に調査できます。

スナップショットがリクエストされるタイミング

アプライアンスの問題でチケットを開くと、特に説明があいまいである場合や問題が断続的に続く場合は、カスタマーサポートからスナップショットを要求される場合があります。特に、次の場合に役立ちます。

- **異常な動作**：スナップショットは、異常時の状態をキャプチャし、サポートに重要な手掛かりを提供します。
- **パフォーマンスの問題**：スナップショット内のリソース使用状況とネットワーク統計を分析すると、ボトルネックや設定の問題を特定できます。

- **ソフトウェアまたはファームウェアの更新**：スナップショットにより、アプライアンスに対する最近の更新の影響を評価できます。

- スナップショットの作成 （46 ページ）

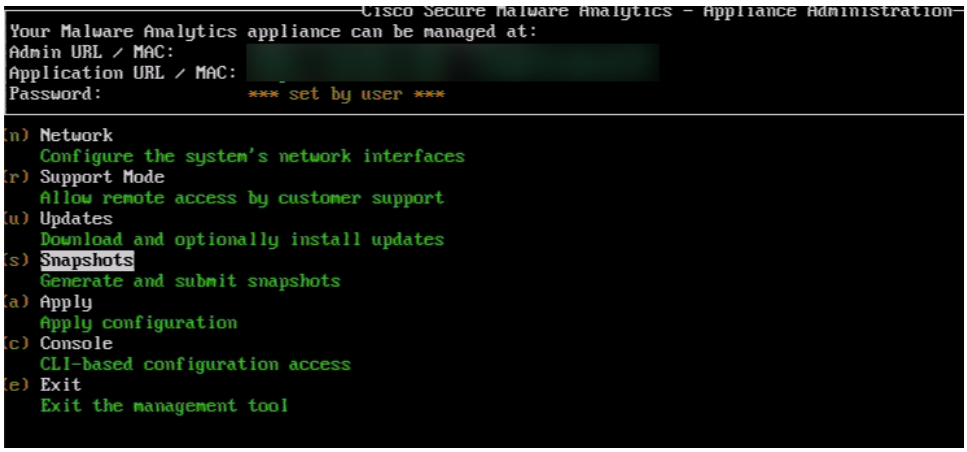
スナップショットの作成

スナップショットを作成するプロセスは次のとおりです。

手順

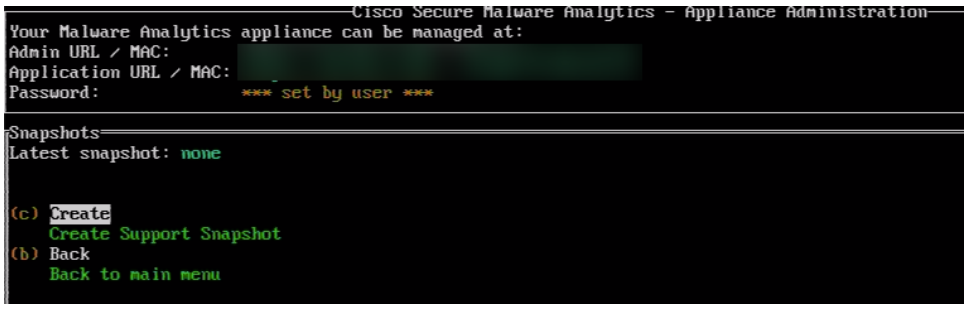
ステップ 1 Admin TUI で、 **[スナップショット（Snapshot）]**を選択します。

図 *18*：スナップショット

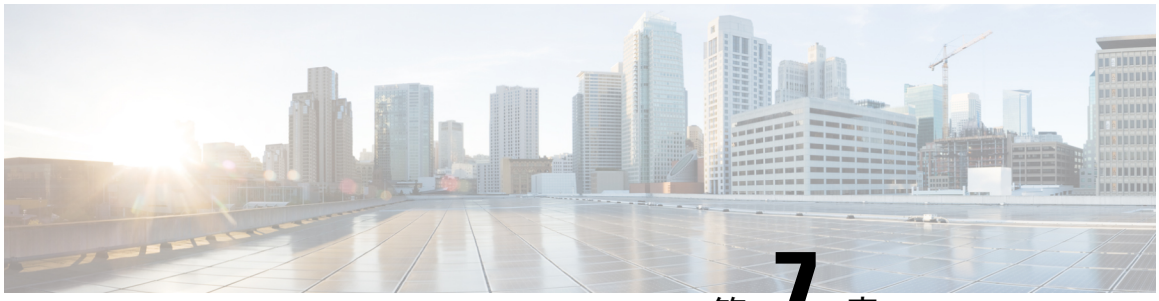


ステップ 2 **[作成（Create）**] オプションを選択すると、スナップショットが生成されます。これで、説明されているプロセスに従って、Admin UI からスナップショットをダウンロードできるようになりました。詳細については、「サポート スナップショット （148 ページ）」を参照してください。

図 *19*：スナップショットの作成



アプライアンスのサイズと複雑さによっては、スナップショットの作成に時間がかかる場合があります。



第 7 章

適用

これが、再構成プロセスをトリガーする重要な要素です。 **[適用（Apply）]**を選択するまで、変更は **非アクティブの** ままで、アプライアンスの動作には影響しません。再構成とは、管理TUI設定で行った変更を実装するプロセスを指します。これには、アプライアンスの実行システムに新しい設定を適用する必要があり、多くの場合、内部リソースやプロセスの調整が必要になります。

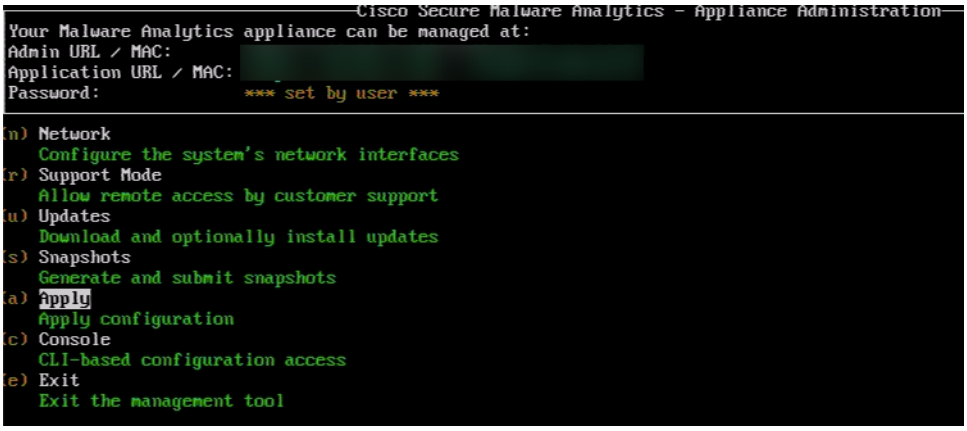
設定を適用する

構成を適用するプロセスは次のとおりです。

手順

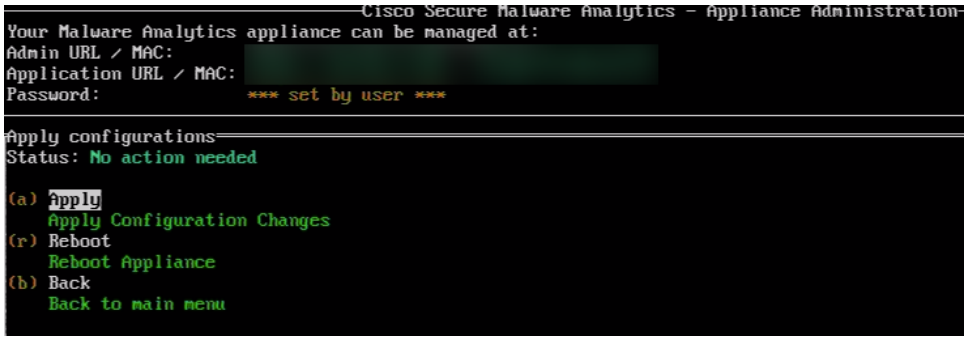
ステップ 1 Admin TUI で、 **[適用（Apply）]**に移動します。

図 *20 :* 適用



ステップ 2 [適用（Apply）] を選択します。

図 *21 : [Apply]* を選択します。



新しい構成を適用します。

アプライアンスの再起動

適用メニュー内で、アプライアンスを再起動できます。

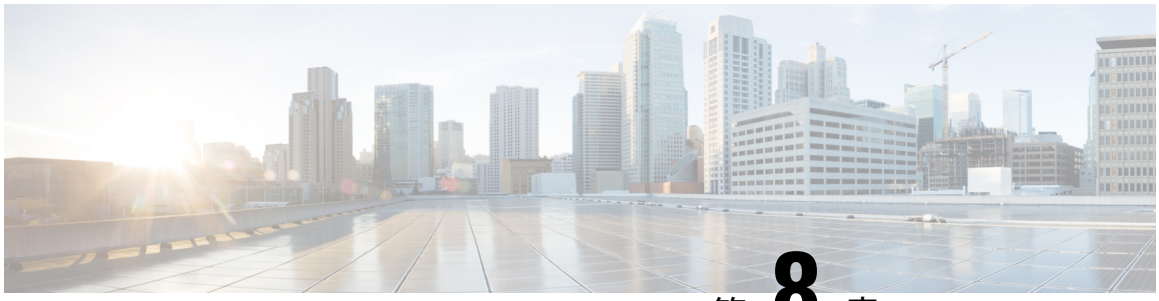
手順

ステップ 1 Admin TUI で、 **適用する**ために移動します。

ステップ 2 [Reboot] を選択します。

（注）
アプライアンスがシャットダウンし、自動的に再起動します。リブートプロセスには数分かかります。完了すると、同じ方法を使用して Admin TUI に再度アクセスできます。

確認メッセージが表示されます。[OK] を選択して、リブートを続行します。



第 8 章

コンソール

コンソールは、上級ユーザーがデバイスのトラブルシューティング、メンテナンス、管理を行うための Admin TUI に搭載された強力なツールです。Admin UI を超えた機能があり、テキストコマンドを介して正確に制御できます。

- コンソールを使用 （49 ページ）

コンソールを使用

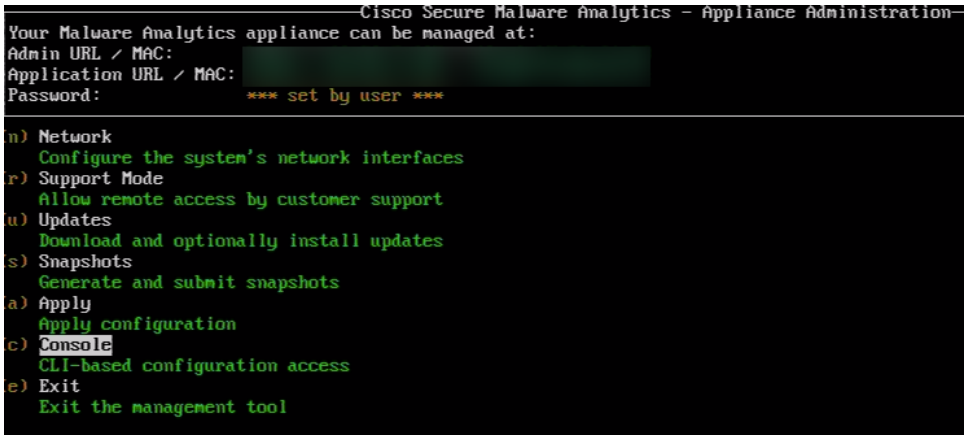
コンソールを使用して、次の操作を実行できます。

- ping または traceroute コマンドによるネットワーク問題のトラブルシューティング。
- 高度な設定タスクの実行。
- サービスの手動再起動

手順

ステップ 1 [管理TUI（Administration TUI）] で、利用可能なオプションから **[コンソール（Console）]** を選択します。

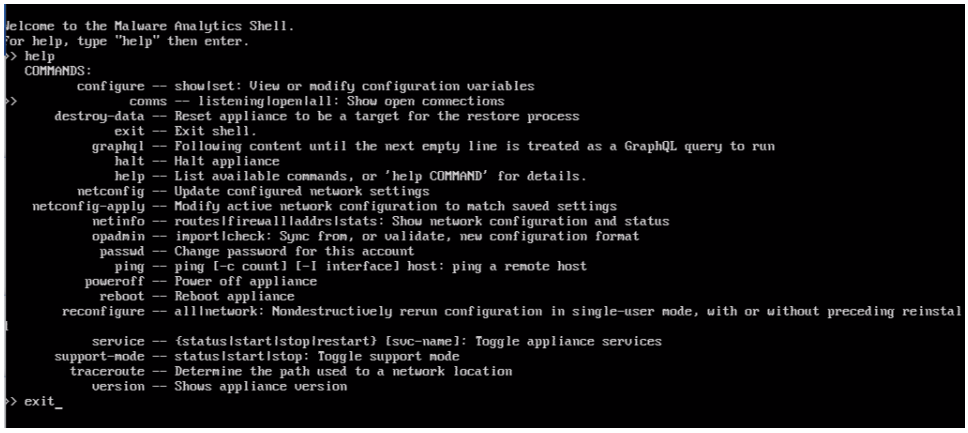
図 *22 :* コンソール



コンソールモードに入り、コマンドを受信できるようになります。

ステップ 2 コマンドを入力して、Enter キーを押して実行します。

図 *23 :* コンソール：コマンド：例

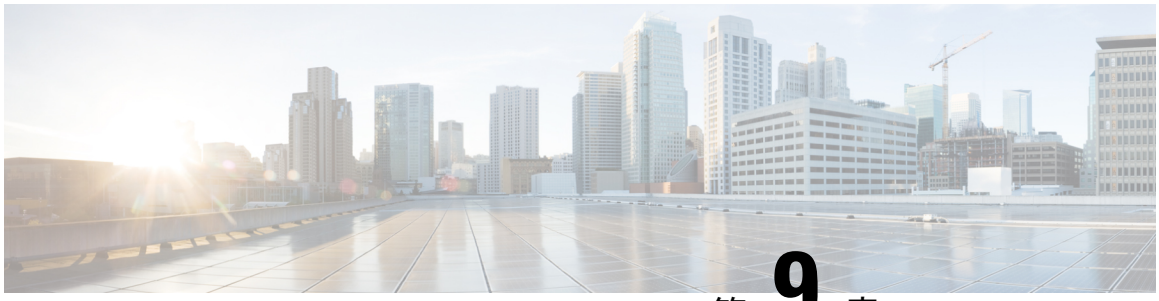


例：

表 *2 :* コマンドの例

コマンド	説明	例
help	使用できるすべてのコマンドをリストします	help
ping	ネットワーク接続をテストします	Ping 8.8.8.8
traceroute	特定の接続先へのパケットのルートを追跡します	traceroute google.com

コマンド	説明	例
exit	コンソールを終了します	exit



第 9 章

終了

[終了（Exit）] オプションを使用すると、Admin TUI からログアウトしてログイン画面に戻ることができます。

- 終了（ログアウト） （53 ページ）

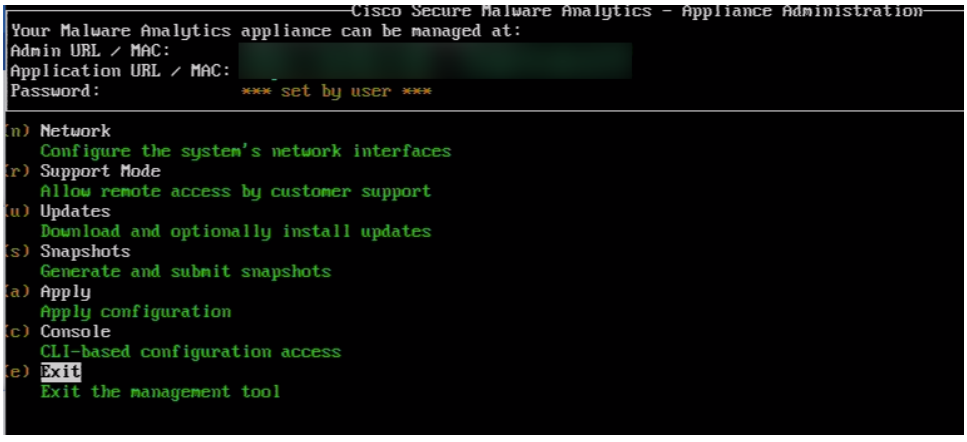
終了（ログアウト）

Admin TUI からの終了：

手順

ステップ 1 Admin TUI で、**[終了（Exit）]**を選択します。

図 *24 :* 終了（*Exit*）



アプリケーションからログアウトすると、ログイン画面が表示されます。

ステップ 2 パスワードを入力し、[Admin TUI] に再度ログインします。

終了（ログアウト）

第 II 部

Admin UI

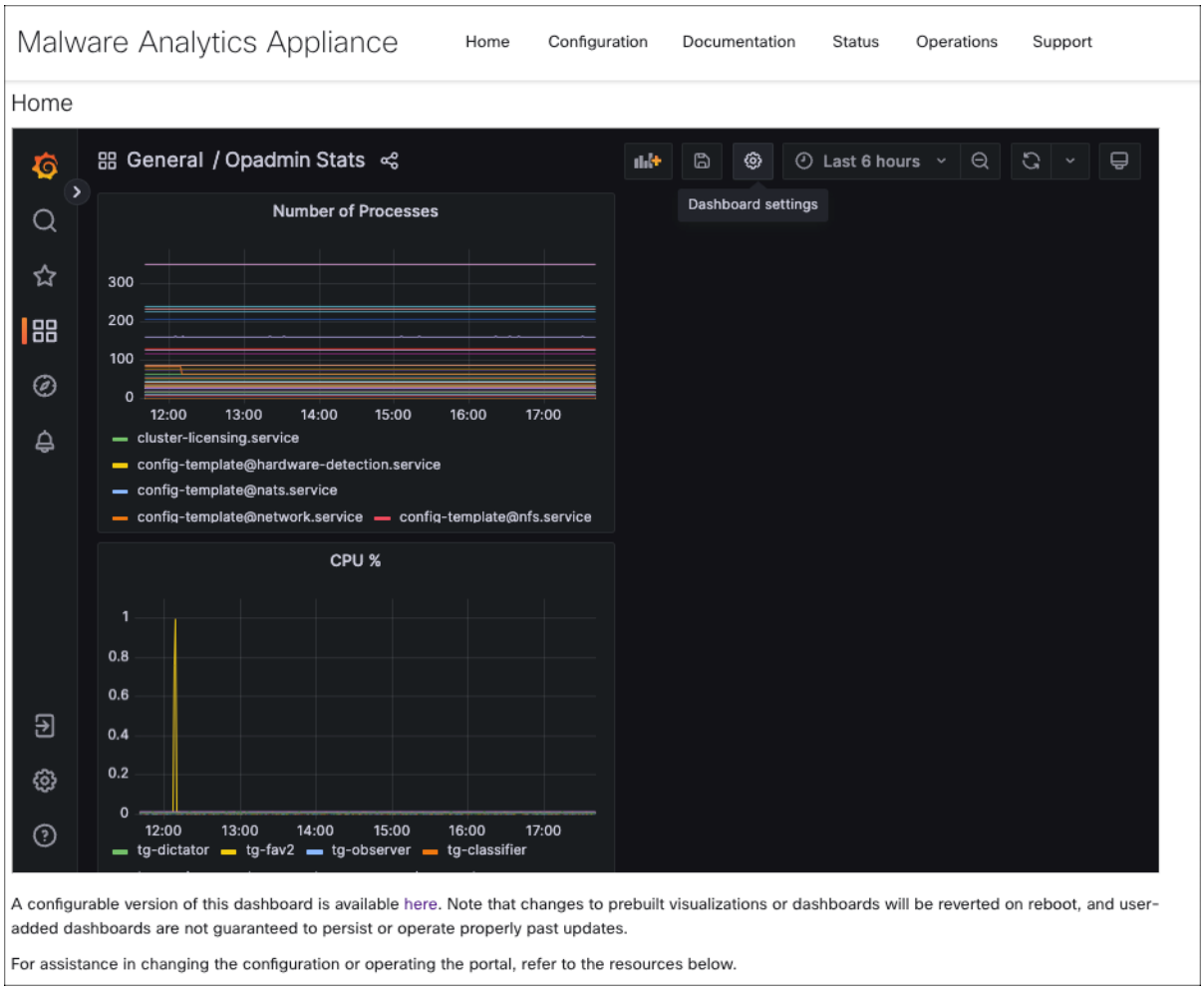
第 10 章

ホーム

システム ダッシュボードがホーム画面に表示され、可視化されるデータ（CPU とプロセス）の時間範囲を管理するための多くの方法が表示されます。ダッシュボードは、管理 UI にログインしたときに最初に表示される画面です。

ホーム

図 *25 : Home*


Malware Analytics Appliance
Home
Configuration
Documentation
Status
Operations
Support
Home
General / Opadmin Stats
Last 6 hours
Dashboard settings
Number of Processes
300
200
100
0
12:00
13:00
14:00
15:00
16:00
17:00
cluster-licensing.service
config-template@hardware-detection.service
config-template@nats.service
config-template@network.service
config-template@nfs.service
CPU %
1
0.8
0.6
0.4
0.2
0
tg-dictator
tg-fav2
tg-observer
tg-classifier
A configurable version of this dashboard is available here. Note that changes to prebuilt visualizations or dashboards will be reverted on reboot, and user-added dashboards are not guaranteed to persist or operate properly past updates.
For assistance in changing the configuration or operating the portal, refer to the resources below.

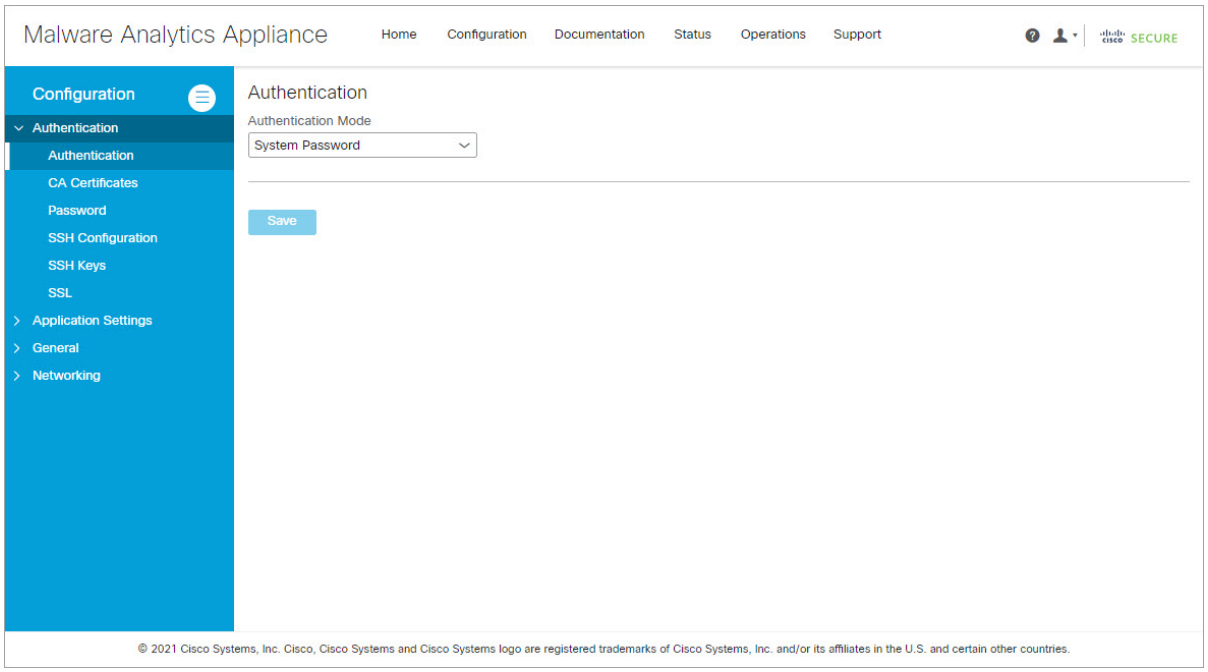
第 11 章

構成

初期設定および構成ウィザードについては、『Cisco Secure Malware Analytics アプライアンスの設定およびコンフィギュレーション ガイド』を参照してください。新しい Secure Malware Analytics アプライアンスでは、管理者が追加の設定を行う必要があります。また、時間の経過に伴い、Admin UI の設定の更新が必要になることがあります。この章では、Admin UI を使用してアプライアンスの設定を変更する方法について説明します。

構成

図 *26 :* 構成



Admin UI の **[構成（Configuration）]** メニューは、次のようなさまざまな Cisco Secure Malware Analytics アプライアンス設定を構成および管理するために使用します。

セクション	説明
Authentication	
認証	Cisco Secure Malware Analytics アプライアンス Admin UI にログインするための LDAP および RADIUS 認証を設定する方法について説明します。
CA 証明書	アプライアンスのアウトバウンド SSL 接続に CA 証明書を追加して Cisco Secure Endpoint プライベートクラウドを信頼する方法について説明します。
パスワード	Admin UI のパスワードを変更する方法について説明します。
SSH の設定 （71 ページ）	SSH を使用していくつかのキー要素をセットアップするための SSH の設定方法について説明します。
SSH キー （72 ページ）	SSH 経由でAdmin TUI にアクセスできるようにするための SSH キーの設定方法について説明します。

セクション	説明
SSL	E メール セキュリティ アプライアンス（ESA）、Web セキュリティ アプライアンス（WSA）、Cisco Secure Endpoint プライベート クラウド、およびその他の統合とのセキュアなマルウェア分析アプライアンスの接続をサポートするための SSL 証明書の構成方法について説明します。 SSL 証明書の置き換え。
アプリケーションの設定	
統合	サードパーティの検出および強化サービス（OpenDNS、Titacloud、VirusTotal）の構成方法について説明します。 ClamAV 自動更新を有効または無効にします。
ライセンス	Cisco Secure Malware Analytics アプライアンスのライセンスをアップロードする方法、またはサーバーからライセンスを取得する方法について説明します。
Network Exit	分析用のサンプルを送信するときに、Cisco Secure Malware Analytics ポータルで使用可能なネットワーク イグジットのオプションを構成する方法について説明します。
プロキシの更新 （90 ページ）	更新をダウンロードするように SOCKS5 プロキシを構成する方法について説明します。
全般	
コンテンツの更新 （91 ページ）	コンテンツ更新を有効にする方法について説明します。
日時	Network Time Protocol（NTP）サーバーを追加して日付と時刻を構成する方法について説明します。
E メール	システム通知の電子メール設定（SMTP）の構成方法について説明します。
通知	通知受信者を管理する方法について説明します。
Syslog	syslog メッセージおよび通知を受信するようにシステム ログ サーバーを設定する方法について説明します。
ネットワーキング	
ネットワーク	DHCP から永続的な静的 IP アドレスへの IP 割り当てを調整する方法と、DNS を構成する方法について説明します。
NFS	NFS 要件、バックアップストレージ要件、バックアップ期待、厳密な保持期間制限の設定など、アプライアンスバックアップについて説明します。バックアップの実行方法。

セクション	説明
クラスタ	Cisco Secure Malware Analytics アプライアンスのクラスタリングの機能、制限事項、および要件について説明します。ネットワークおよびNFS ストレージの要件クラスタの構築、クラスタへのアプライアンスの参加、クラスタノードの削除、タイ ブレーカー ノードの指定方法。耐障害性と障害回復クラスタの API と運用の使用方法と特性、および削除例の詳細を表示します。

（注）

- 構成時に IP アドレスが遮断される可能性を減らすために、Admin UI での構成の更新は 1 回のセッションで完了する必要があります。
- Admin UI はゲートウェイ エントリを検証しません。誤ったゲートウェイを入力して保存すると、Admin UI にアクセスできなくなります。ネットワーク設定を管理インターフェイスで実行した場合は、コンソールを使用してネットワーク設定を修正する必要があります。Admin がまだ有効であればい、Admin UI でそれを修正して、再起動できます。
- Cisco Secure Malware Analytics アプライアンス（v2.7 以降）は、ホスト名としてシリアル番号を使用することにより、一部の NFS v4 サーバーとの相互運用性を向上させます。

重要

Admin UI は HTTPS を使用するため、ブラウザのアドレスバーに HTTPS を入力する必要があります。Admin IP をポイントするだけでは十分ではありません。ブラウザに次のアドレスを入力します。

https://adminIP/

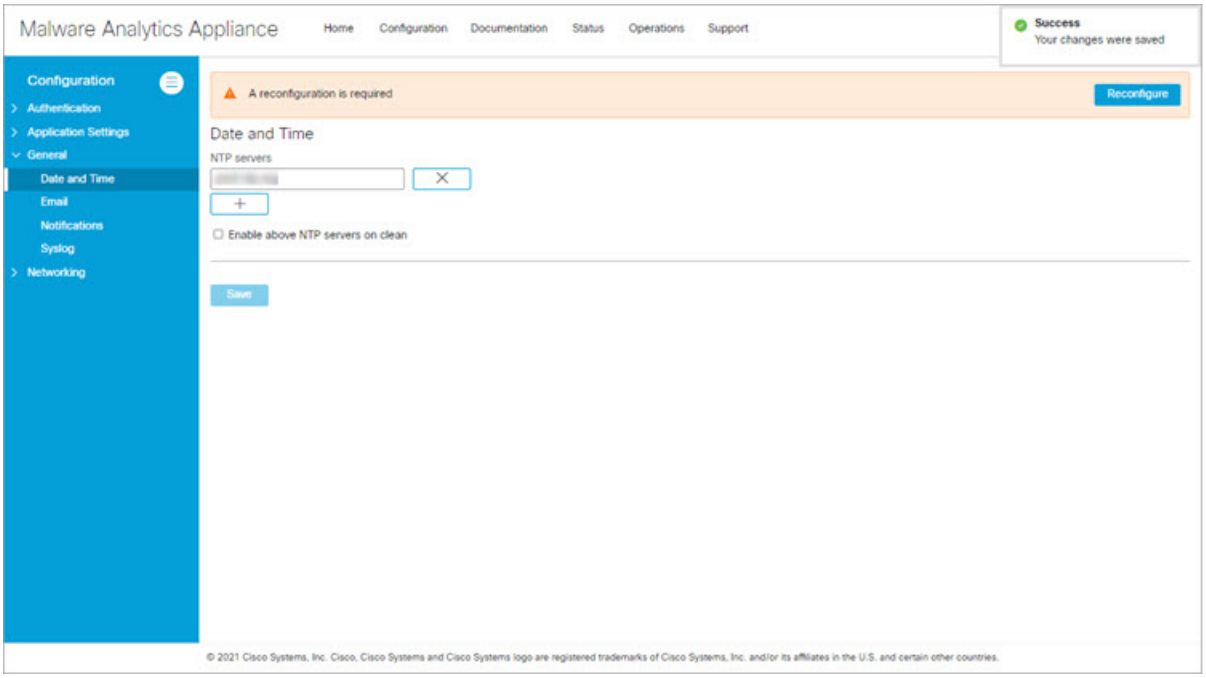
または

https://adminHostname/

構成変更の適用

構成の設定に変更が加えられるたびに、**[構成（Configuration）]** ページの上部にあるバナーに、薄いオレンジ色のアラート メッセージが表示されます。

図 *27 :* 必要なアラート メッセージの再構成



Admin UI の構成に対する変更は、保存する必要があり、いくつかには変更をアクティブ化する手順も含まれています。ただし、別の手順で再構成して変更を確定する必要もあります。設定の変更は、再構成が完了するまで有効になりません。

（注） 再構成すると、Cisco Secure Malware Analyticsポータルおよび Admin UIにログインしている他のユーザーに影響を与える可能性があります。

手順

ステップ 1 アラートメッセージの **[再構成（Reconfigure）]** をクリックして、再構成プロセスを開始します。それ以外の場合は、再構成するには、 **[操作（Operations）]** > **[アクティブ化（Activate）]**をクリックします。

ステップ 2 **[構成のアクティブ化（Activate Configuration）]** ページで、 **[再構成（Reconfigure）]** をクリックして再構成ジョブを実行します。

ステップ 3 確認ダイアログで、 **[再構成（Reconfigure）]** をクリックして再構成ジョブを開始します。

構成がアクティブ化され、その進行状況に関するメッセージが [ジョブ（Jobs）] ウィンドウに表示されます。エラー メッセージやその他の情報を確認する必要がある場合は、詳細が **[ジョブ（Jobs）]** ページに保持されます。

完了すると、再構成が成功したことを示す確認メッセージが表示されます。

ステップ 4 [Continue] をクリックします。

認証

Cisco Secure Malware Analytics アプライアンスでは、管理 UI および管理 TUI にログインするための LDAP 認証および許可がサポートされています。また、RADIUS 認証もサポートされています。これにより、v2.10 以降で管理 UI にシングルサインオンが可能になります。

LDAP 認証

Secure Malware Analytics アプライアンスでは、管理 UI および管理 TUI ログインの LDAP 認証および許可がサポートされています。ドメインコントローラまたは LDAP サーバーで管理されるさまざまなログイン情報を使用して、複数のアプライアンス管理者を認証できます。認証モードは、[System Password Only]、[System Password or LDAP]、[LDAP Only] のいずれかです。

3 つの LDAP プロトコル オプション、[LDAP]、[LDAPS]、[LDAP with STARTLS] があります。

次の点を考慮する必要があります。

- デュアル認証モード（**LDAP またはシステム パスワード**）は、LDAP の設定時に、Secure Malware Analytics アプライアンスから誤ってロックアウトされないようにするために必要です。

  最初から [**LDAP のみ（LDAP Only**）] を選択することはできません。まずデュアルモードを実行して、動作することを確認する必要があります。初期設定後に Admin UI からログアウトした後、LDAP ログイン情報を使用して再度ログインして [**LDAP Only**] に切り替える必要があります。

- 認証を [**LDAP のみ（LDAP Only**）] に設定した場合、Admin TUI ダイアログにログインするには LDAP を使用する必要があります。認証モードが [**LDAP またはシステム パスワード（LDAP or System Password**）] に設定されている場合、Admin TUIのログインで許可されるのはシステム ログインのみです。

- Secure Malware Analytics アプライアンスが LDAP 認証のみ（[**LDAP のみ（LDAP Only**）]）に設定されている場合は、リカバリ モードでパスワードをリセットして、認証モードを再設定し、システムパスワードによるログインを許可することもできます。

- メンバーシップを制限するための認証フィルタが設定されていることを確認します。

- Admin TUI と Admin UI では、[**LDAP のみ（LDAP Only**）] モードの場合にのみ LDAP ログイン情報が必要です。[**LDAP のみ（LDAP Only**）] に設定されている場合、Admin TUI では、システム パスワードではなく、LDAP ユーザー/パスワードの入力のみが求められます。

- 認証が [**システム パスワードまたは LDAP（System Password or LDAP**）] に設定されている場合、Admin TUI では、これら両方ではなく、システムパスワードのみを入力するように求められます。

- LDAP の問題をトラブルシューティングするには、リカバリモードでパスワードをリセットして LDAP を無効にします。
- SSH を使用して Admin TUI ダイアログにアクセスするには、[**LDAP のみ（LDAP Only**）] モードの場合、LDAP ログイン情報に加えて、システムパスワードまたは設定済みの SSH キーが必要です。
- LDAP はクリーン インターフェイスからの発信です。

Admin UI で LDAP 認証を構成するには、次の手順を実行します。

手順

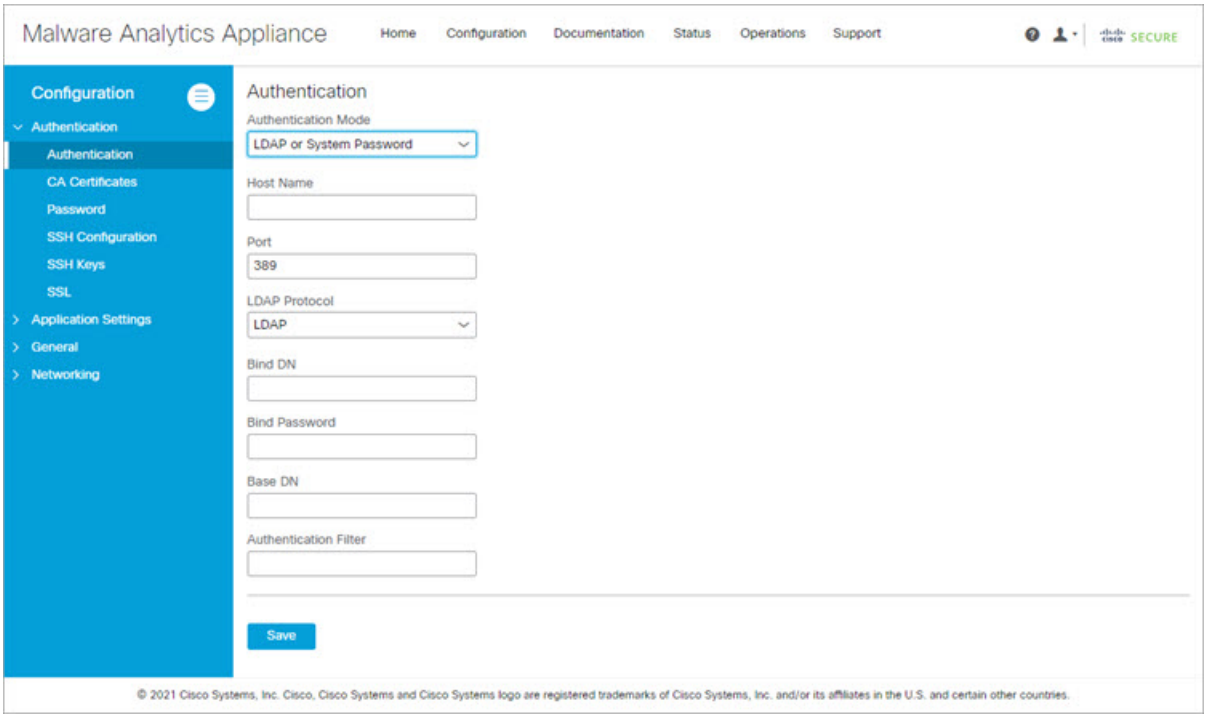
ステップ 1 [構成（Configuration）] タブをクリックします。

ステップ 2 サイドナビゲーションで **[認証（Authentication）]** を展開し、 **[認証（Authentication）]**を選択します。

ステップ 3 **[認証モード（Authentication Mode）]** ドロップダウンから **[LDAP] または [システムパスワード（System Password）]** を選択して、[LDAP 設定（LDAP configuration）] ページを開きます。

（注）
LDAP 認証を最初に構成するときは、[**LDAP またはシステム パスワード（LDAP or System Password)**] を選択し、Admin UI からログアウトしてから、LDAP ログイン情報を使用して再度ログインする必要があります。その後、 [**LDAP**] を実装するように設定を変更できます。

図 *28 : [LDAP* 認証構成（*LDAP Authentication Configuration***）*]* ページ**



ステップ 4 適宜、ページのフィールドに入力します。

- **ホスト名（Hostname）**：LDAP 経由で接続するホスト名。
- **[ポート（Port）]**：LDAP 経由で接続するポート番号（デフォルトは 389）。
- **[認証モード（Authentication Mode）]**：ログイン時に使用される認証モード。
- **[LDAP プロトコル（LDAP Protocol）]**：使用されている LDAP プロトコル。
- **[バインド パスワード（Bind Password）]**：LDAP 経由のバインドに使用するパスワード。
- **[バインド DN（Bind DN）]**：LDAP 経由でバインドするための識別名。例：cn=admin,dc=foo,dc=com。
- **[ベース（Base）]**：LDAP 経由でバインドするベース。例：ou=users,dc=foo,dc=com（LDAP のみ）。
- **[認証フィルタ（Authentication Filter）]**：ログイン時の認証に適用されるフィルタ。例：(&(cn=%LOGIN%) (memberOf=cn=admingroup, ou=groups,dc=foo,dc=com))。

ステップ 5 [保存（Save）] をクリックします。

ユーザーは管理 UI または管理 TUI にログインすると、LDAP 認証を求められます。

RADIUS 認証

Cisco Secure Malware Analytics アプライアンス（v2.10 以降）は、DTLS が有効な Cisco Identity Services Engine を使用する RADIUS 認証をサポートしています。RADIUS 認証が有効になっている場合、ユーザーは適切なシングル サインオン パスワードを使用して、メインの Secure Malware Analytics アプリケーション UI および OpAdmin にログインできます。

次の点を考慮する必要があります。

- デュアル認証モード（**RADIUS またはシステム パスワード**）は、RADIUS の設定時に、Secure Malware Analytics アプライアンスから誤ってロックアウトされないようにするために必要です。

  最初から [**RADIUS のみ（RADIUS Only）**] を選択することはできません。まずデュアルモードを実行して、動作することを確認する必要があります。初期設定後に Admin UI からログアウトした後、RADIUS ログイン情報を使用して再度ログインして **[RADIUS のみ（RADIUS Only）]** に切り替える必要があります。

- **[RADIUS のみ（RADIUS Only）**] 認証に設定されている場合のみ、RADIUS を使用して管理 TUI にログインできます。認証モードが [**RADIUS またはシステム パスワード（RADIUS or System Password）**] に設定されている場合、Admin TUIのログインで許可されるのはシステム ログインのみです。

- Secure Malware Analytics アプライアンスが RADIUS 認証のみ（[**RADIUS のみ（RADIUS Only）**]）に設定されている場合は、リカバリ モードでパスワードをリセットして、認証モードを再設定し、システムパスワードによるログインを許可することもできます。

- 管理 TUI および管理 UI は **[RADIUS のみ（RADIUS Only）]** モードでのみ RADIUS ログイン情報を必要とします。**RADIUS のみが** 設定されている場合、管理 TUI は RADIUS ユーザー/パスワードのプロンプトのみを表示します。システムパスワードではありません。
- 認証が [**RADIUS またはシステム パスワード（RADIUS or System Password**）] に設定されている場合、Admin TUI では、これら両方ではなく、システム パスワードのみを入力するように求められます。
- RADIUS の問題をトラブルシューティングするには、リカバリモードでパスワードをリセットして LDAP を無効にします。
- SSH を使用して Admin TUI ダイアログにアクセスするには、[**RADIUS のみ（RADIUS Only**）] モードの場合、RADIUS ログイン情報に加えて、システム パスワードまたは設定済みの SSH キーが必要です。
- RADIUS はクリーン インターフェイスからの発信です。

Admin UI で RADIUS 認証を構成するには、次の手順を実行します。

手順

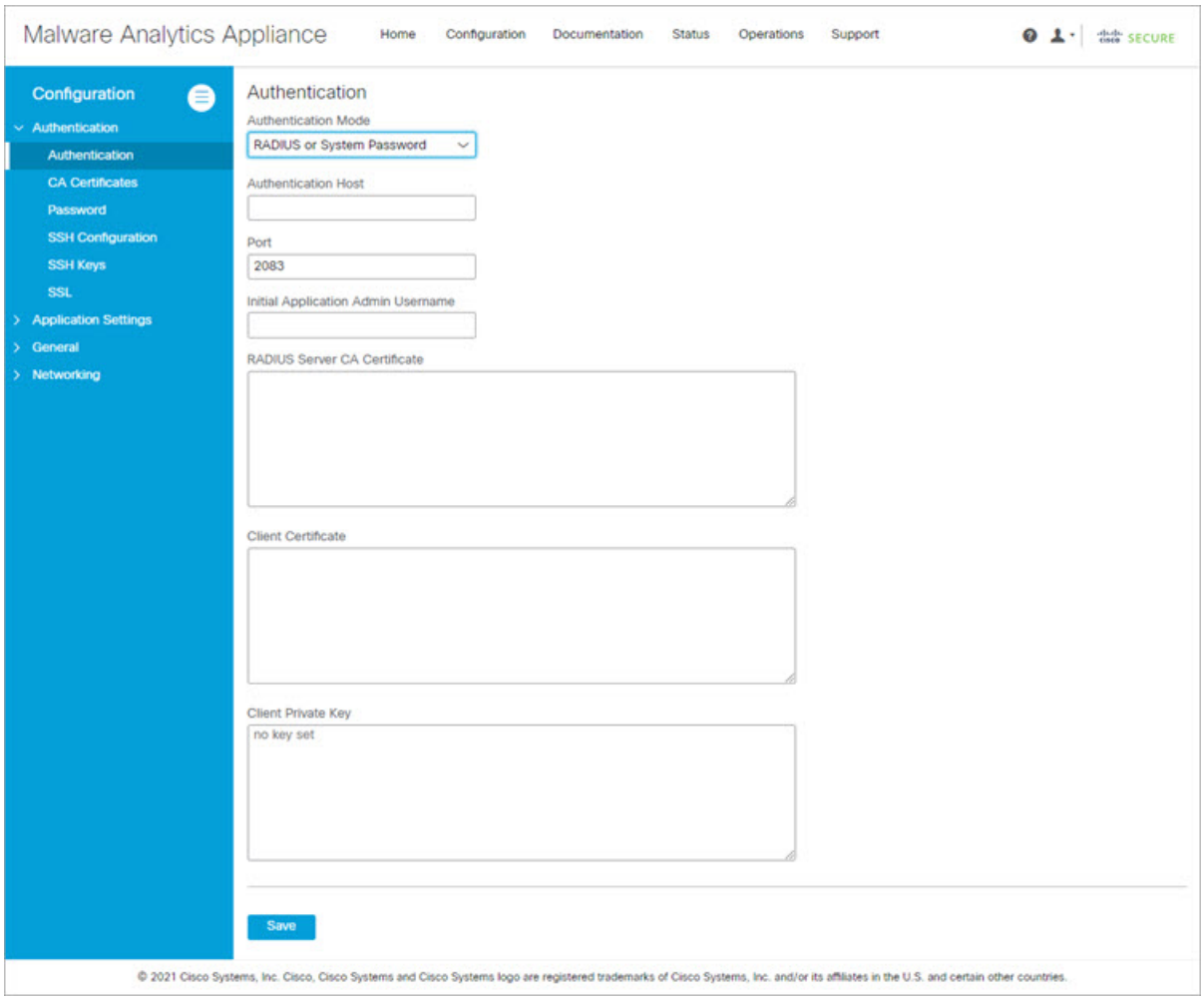
ステップ 1 [構成（Configuration）] タブをクリックします。

ステップ 2 サイド ナビゲーションで **[認証（Authentication）]** を展開し、 **[認証（Authentication）]**を選択します。

ステップ 3 **[認証モード（Authentication Mode）]** ドロップダウンから **[RADIUS] または [システム パスワード（System Password）]** を選択して [RADIUS設定（RADIUS configuration）] ページを開きます。

（注）
RADIUS 認証を最初に構成するときは、[**RADIUS またはシステム パスワード（RADIUS or System Password)**] を選択し、Admin UI からログアウトしてから、LDAP ログイン情報を使用して再度ログインする必要があります。その後、設定を **[RADIUS]**に変更できます。RADIUS とシステム パスワードを設定した後に 2 回めのログインを行うと、フォールバック ログイン方式としてシステム パスワードを削除する前に RADIUS の設定が検証されます。

図 *29 : [RADIUS* 認証構成（*RADIUS Authentication Configuration*）*]* ページ



ステップ 4 適宜、ページのフィールドに入力します。

- **ホスト名** ：RADIUS 経由で接続するホスト名。
- **[ポート（Port）]**：RADIUS 経由で接続する DTLS ポート番号（デフォルトは 2083）。従来の RADIUS とは異なり、DTLS では認証とアカウンティングの両方に単一のポートを使用します。DTLS ベースの RADIUS 認証のみがサポートされています。
- **最初の管理者** ：プライマリ Cisco Secure Malware Analytics UI の初期/デフォルトの管理ユーザーがマッピングされる RADIUS ユーザー。このアカウントは、Cisco Secure Malware Analytics で他のユーザーアカウントを作成し、権限を設定する当事者である必要があります。
- **[CA証明書（CA Certificate）]**：認証に使用される RADIUS サーバーの認証に使用する PEM 形式の CA 証明書。次に変更します<VALID>正常に保存されました。フィールドを空にするには、これをクリアします。

- **クライアント証明書**：認証に使用される RADIUS サーバに対してこのホストを認証するために使用する PEM 形式のクライアント証明書。この値は次に変更されます。<VALID>正常に保存されたとき。これをクリアしてフィールドを空にすることができます。
- **[クライアント秘密キー（Client Private Key）]**：認証に使用される RADIUS サーバーに対して、このホストを認証するために使用する PEM 形式のキー。この値は、上記のクライアント証明書に対応している必要があります。値が次に変更されます<VALID>正常に保存されたとき。これをクリアしてフィールドを空にすることができます。新しい管理 UI では、PEM エンコード PKCS#8 形式の秘密キーがサポートされています。

ステップ 5 [保存（Save）] をクリックします。

（注）
`NAS 識別子`は、Security Malware Analytics UI および OpAdmin からの認証要求で送信されます。

- SMA ポータルからの認証要求で送信される`NAS 識別子`は次のとおりです： `Threat Grid UI`。
- OpAdmin からの認証要求で送信される`NAS 識別子`は次のとおりです：`Threat Grid Admin`。

`NAS-identifier`を介して送信される特定の値の詳細については、 https://www.rfc-editor.org/rfc/rfc2865.html#section-5.32を参照してください。

CA 証明書

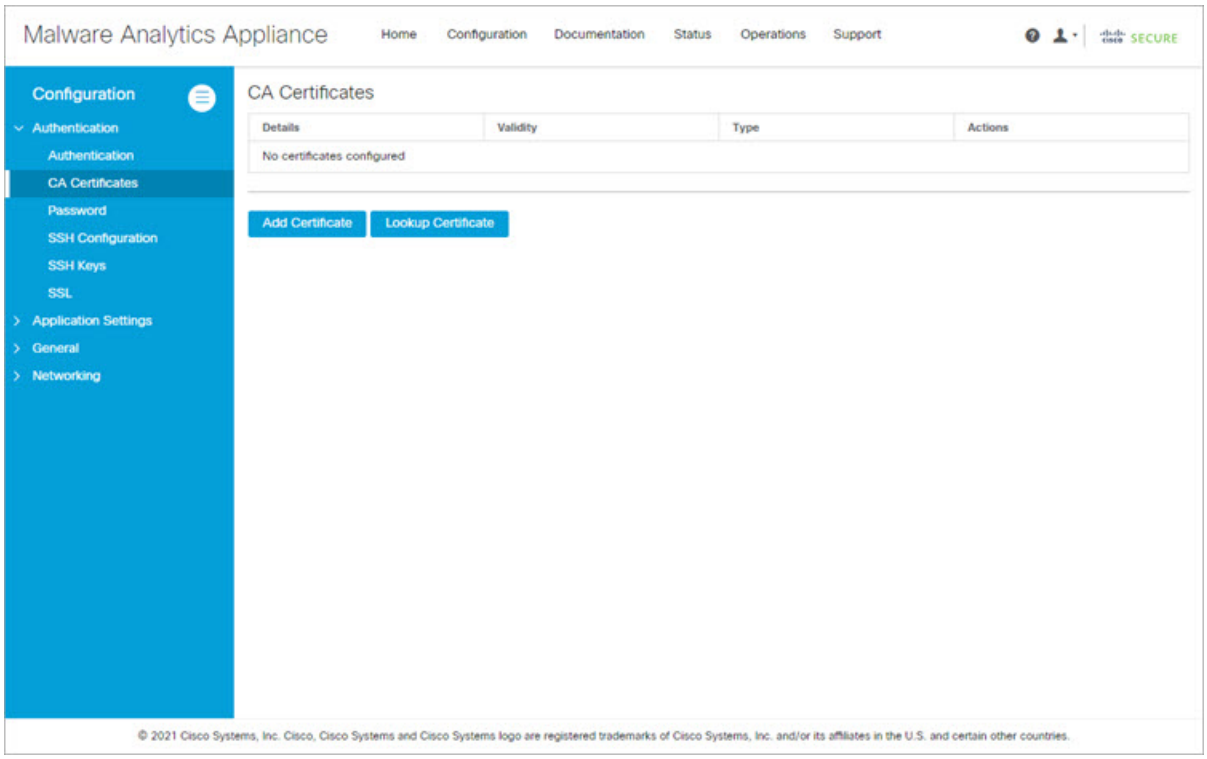
Admin UI の [**CA Certificate**] ページは、アウトバウンド SSL 接続用の CA 証明書信頼ストアを管理するために使用されるため、Secure Malware Analytics アプライアンスは、Cisco Secure Endpoints プライベート クラウドを信頼して、悪意があると見なされた分析済みサンプルについて通知することができます。

手順

ステップ 1 [構成（Configuration）] タブをクリックします。

ステップ 2 サイドナビゲーションで **[認証（Authentication）]** を展開し、 **[CA 証明書（CA Certificates）]** を選択して **[CA 証明書（CA Certificates）]** ページを開きます。

図 *30 : [CA* 証明書（*CA Certificates*）*]* ページ



ステップ 3 Cisco Secure Endpoint プライベートクラウドのアウトバウンド SSL 接続（CA 証明書）を含む **.pem** ファイルを作成し、内容をコピーして **[証明書 （Certificate）]** フィールドに貼り付けます。

ステップ 4 **[証明書の追加（Add Certificate）]** をクリックして確認します。CA 証明書を変更しても、再構成は必要ありません。

パスワード

アプライアンス パスワードを、Cisco Secure Malware Analyticsアプライアンス Admin UI とアプライアンス コンソールへの認証に使用します。 **[Password]** ページを使用して、Admin UI からパスワードを変更できます。

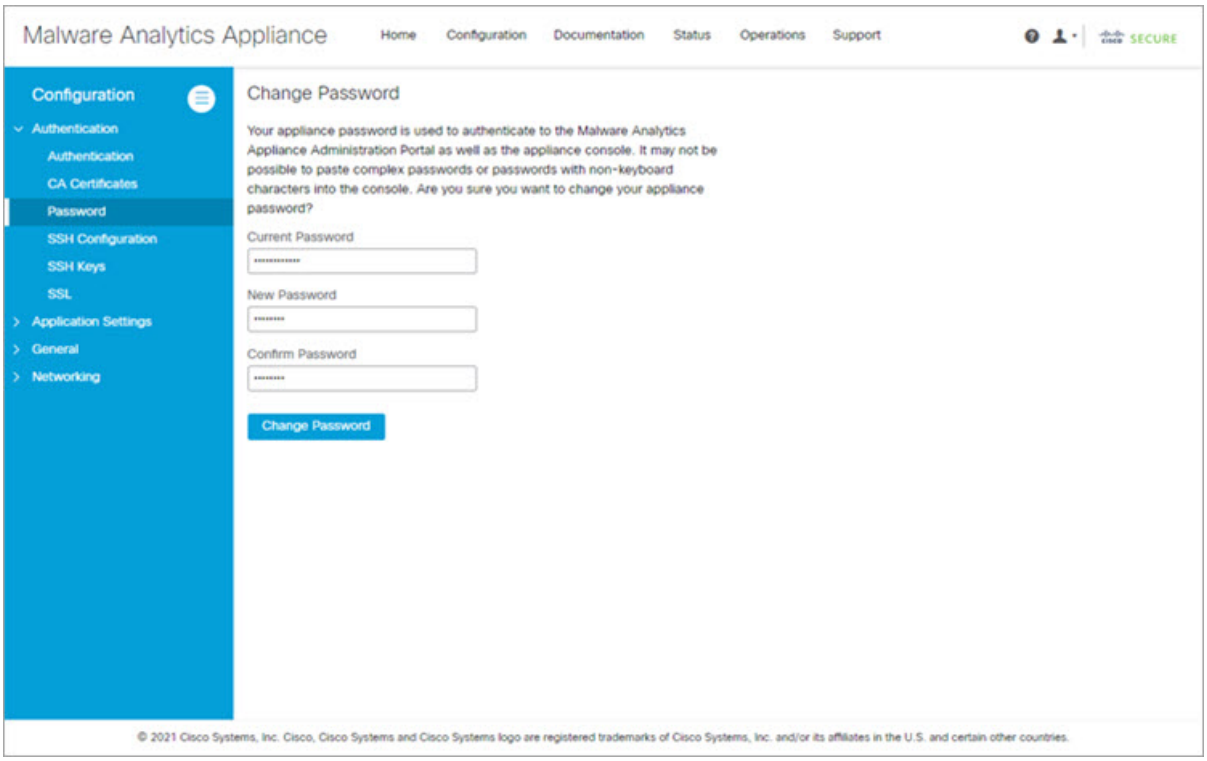
（注） キーボードにない文字を使用した複雑なパスワードは、コンソールに貼り付けられない場合がありますので、パスワードの変更の際には気を付けてください。

手順

ステップ 1 [構成（Configuration）] タブをクリックします。

ステップ 2 サイドナビゲーションで **[認証（Authentication）]** を展開し、 **[パスワード（Password）]**を選択します。

図 *31* : パスワード



ステップ 3 **現在のパスワード**、**新しいパスワード**を入力し、**パスワードを確認**を入力します。

ステップ 4 **[パスワードの変更（Change Password）]** をクリックし、変更を確認します。パスワードを変更しても、再構成の必要はありません。

SSH の設定

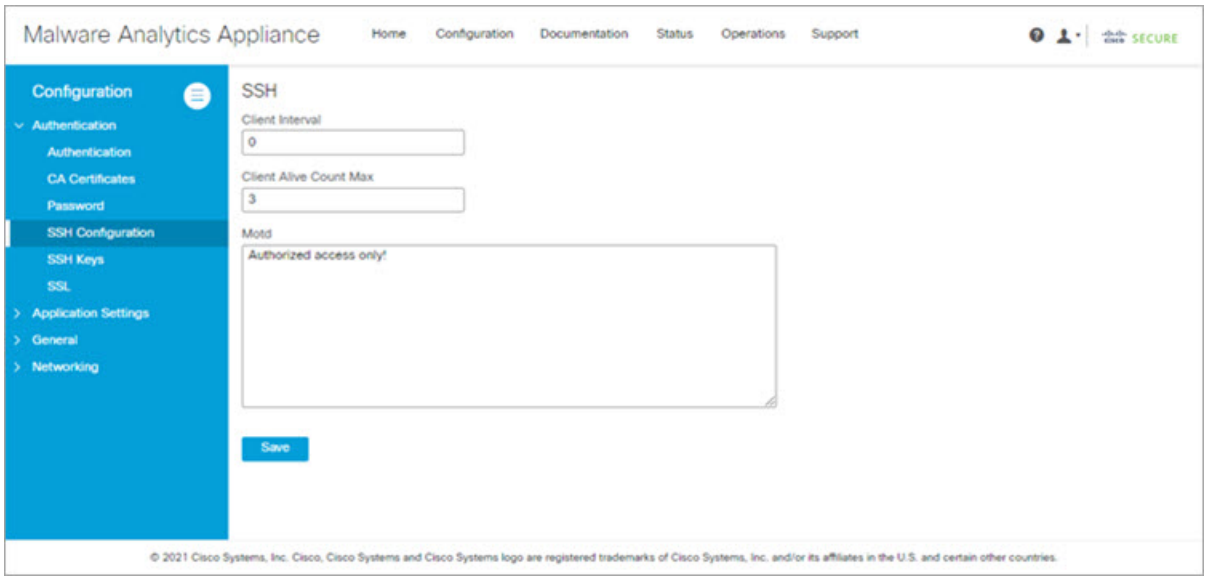
[SSH 設定（SSH Configuration）] を設定すると、Cisco Secure Malware Analytics アプライアンス管理者は、管理 UI の **[SSH設定（SSH Configuration）]** ページを使用して、アプライアンスで *ClientAliveInterval*、 *ClientAliveCountMax* 、および *motd* （Message of the Day）を設定するためのアクセス権が付与されます。

手順

ステップ 1 [構成（Configuration）] タブをクリックします。

ステップ 2 サイドナビゲーションで **[Authentication]** を展開し、 **[SSH Configuration]** を選択して **[SSH Configuration]** ページを開きます。

図 *32 : SSH* の設定



ステップ 3 **[クライアント間隔（Client Interval）]**を入力します。*Client Interval* または *ClientAliveInterval* コマンド：タイムアウト間隔を秒単位で設定します。この時間が経過してもクライアントからデータが受信されない場合、sshd は暗号化されたチャネルを介してメッセージを送信し、クライアントからの応答を要求します。デフォルトは 0 で、これらのメッセージはクライアントに送信されません。

ステップ 4 **[Client Alive Count Max]**を入力します。*Client Alive Count Max* または *ClientAliveCountMax*：SSH がクライアントからメッセージを受信せずに送信されるクライアントアライブメッセージの数を設定します。クライアントアライブメッセージの送信中にこのしきい値に達すると、sshd はクライアントを切断し、セッションを終了します。

ステップ 5 **Motd** (本日のメッセージ) を入力します。リモートユーザーが SSH を使用して Cisco Secure Malware Analytics アプライアンスにログインしたときに、メッセージを表示するために使用されます。

SSH キー

SSH キーを設定すると、Cisco Secure Malware Analytics アプライアンスの管理者は、SSH を介して管理 TUI にアクセスできます（`threatgrid@`<host>）。ルートアクセスまたはコマンドシェルは提供しません。管理 UI の **[SSHキー（SSH keys）]** ページを使用して、アプライアンスで SSH キーを追加およびリモートできます。

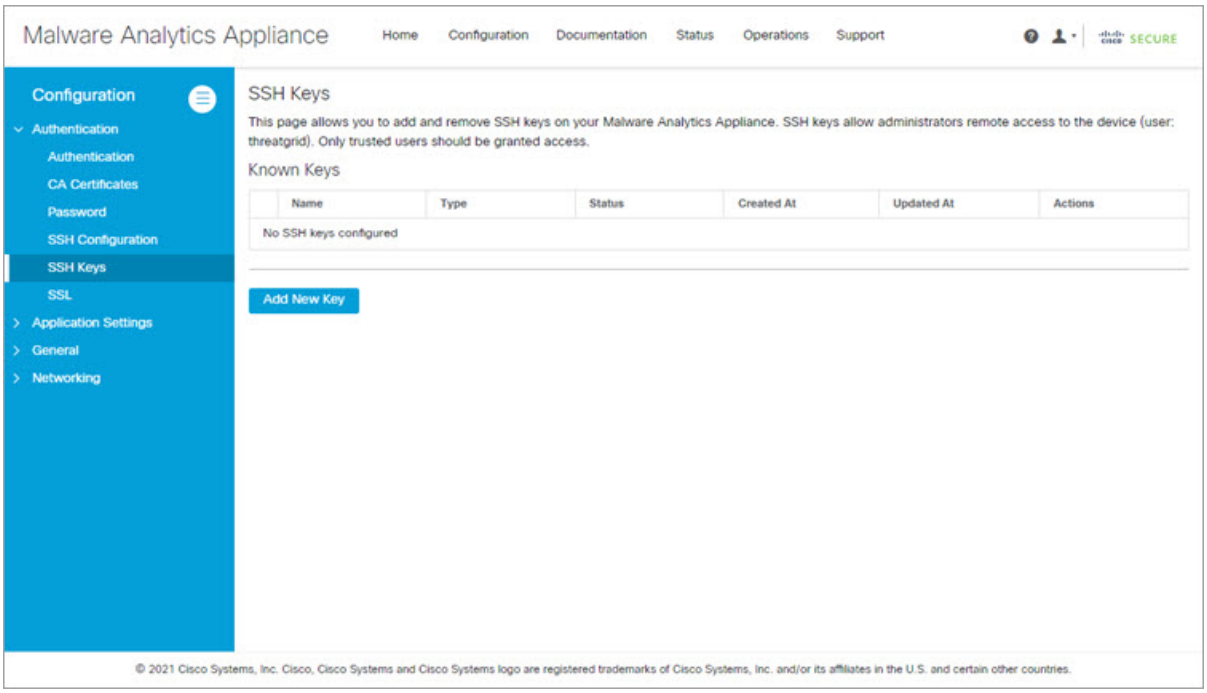
（注） Cisco Secure Malware Analytics アプライアンスにアクセスするための SSH 公開キーを設定すると、SSH を使用したパスワードベースの認証が無効になります（v2.7.2 以降）。そのため、2 つの SSH 認証方式は、両方ではなくどちらか一方のみが有効になります。キーベース認証を使用して SSH 接続が成功すると、Admin TUI プロンプトで、両方のトークンが必要なパスワードの入力を求められます。

手順

ステップ 1 [構成（Configuration）] タブをクリックします。

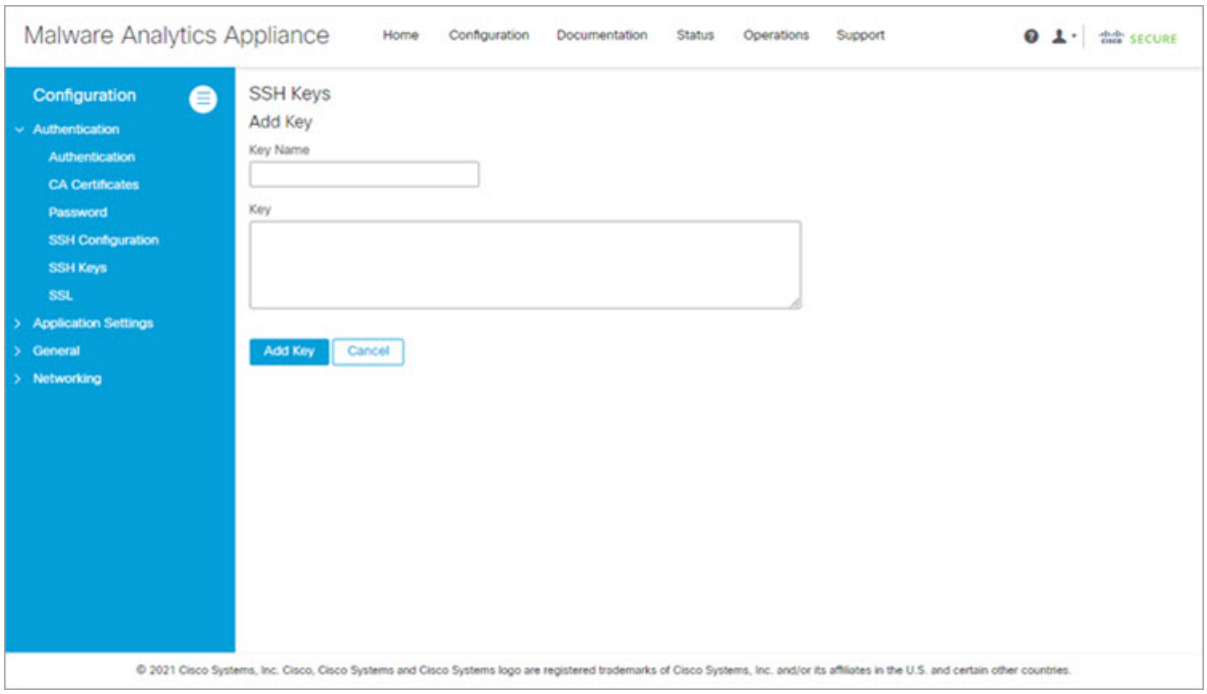
ステップ 2 サイドナビゲーションで **[認証（Authentication）]** を展開し、**[SSHキー（SSH keys）]** を選択して **[SSHキー（SSH keys）]** ページを開きます。

図 *33 : SSH* キー



ステップ 3 **[新しいキーを追加（Add New Key）]** をクリックします。

図 *34* : キーの追加



ステップ 4 **[キー名（Key Name）]** を入力し、キーを **[キー（Key）]** フィールドに貼り付けます。

ステップ 5 [キーを追加（Add Key）] をクリックします。

SSL

Cisco Secure Malware Analytics アプライアンスを通過するネットワーク トラフィックは、SSL を使用してすべて暗号化されます。次の情報は、E メール セキュリティ アプライアンス（ESA）、Web セキュリティアプライアンス（WSA）、Secure Endpoints プライベートクラウドといった統合先との Cisco Secure Malware Analytics アプライアンスの接続をサポートするように SSL 証明書を設定する手順の実行に役立ちます。

（注） SSL 証明書を管理する方法の詳細は、このガイドの説明範囲に含まれていません。

SSL を使用するインターフェイス

Cisco Secure Malware Analytics アプライアンスには、SSL を使用する 2 つのインターフェイスがあります。

- Cisco Secure Malware Analytics ポータルの UI と API、および統合先（ESA/WSA アプライアンス、Secure Endpoint プライベートクラウド配置更新サービス）用の**クリーン**インターフェイス。

- Admin UI の**管理**インターフェイス。

サポートされている SSL/TLS バージョン

Cisco Secure Malware Analytics アプライアンスでは、次のバージョンの SSL/TLS がサポートされています。

- TLS v1.0：管理インターフェイスでは無効（v2.7 以降）
- TLS v3.0：管理インターフェイスでは無効（v2.7 以降）
- TLS v1.2

（注） TLS v1.0 と TLS v3.0 は、管理インターフェイスでは無効になっており（v2.7 以降）、メインアプリケーションでもデフォルトでは無効になっています。これらのプロトコルのいずれかが統合の互換性のために必要な場合は、tgsh から再有効化できます（メインアプリケーションの場合のみ）。

サポートされているお客様提供の CA 証明書

お客様提供の CA 証明書がサポートされており（v2.0.3 以降）、お客様独自の信頼できる証明書または CA 証明書をインポートすることができます。

自己署名デフォルト SSL 証明書

Cisco Secure Malware Analytics アプライアンスは、自己署名 SSL 証明書とキーのセットがインストールされて出荷されます。1 つのセットがクリーン インターフェイス用で、もう一つのセットが管理インターフェイス用です。管理者はこれらの SSL 証明書を置き換えることができます。

デフォルトの Cisco Secure Malware Analytics アプライアンスの SSL 証明書のホスト名（共通名）は、アプライアンスのシリアル番号（IP アドレスの追加の subjectAltName フィールドを持つ）で、1 年間有効です。v2.11 より前のリリースでは、デフォルトの SSL 証明書のホスト名は **pandem** です。

設定時に別のホスト名が Cisco Secure Malware Analytics アプライアンスに割り当てられた場合、証明書内のホスト名と共通名は一致しなくなります。

証明書内のホスト名は、接続先の ESA や WSA、または他の統合先のシスコデバイスやサービスによって想定されるホスト名とも一致している必要があります。多くのクライアントアプリケーションは、証明書で使用される共通名が接続するアプライアンスのホスト名と一致する SSL 証明書を必要とするためです。

SSL 証明書の構成

ESA、WSA、Cisco Secure Endpoint プライベートクラウドなどのシスコのセキュリティ製品は、Cisco Secure Malware Analytics アプライアンスに接続（インバウンド接続）して、サンプルを

送信できます。これを実現するには、接続されるアプライアンスまたは他のデバイスが Cisco Secure Malware Analytics アプライアンスの SSL 証明書を信頼できる必要があります。

まず、ホスト名が共通名と一致していることを確認する必要があります。一致していない場合は、再生成するか置き換える必要があります。その後、Cisco Secure Malware Analytics アプライアンスから SSL 証明書をエクスポートし、接続されるアプライアンスまたはデバイスにインポートする必要があります。

インバウンド SSL 接続に使用される Threat Grid アプライアンスの証明書は、[**SSL Certificate**] ページで設定されます。クリーン インターフェイスと管理インターフェイス用の SSL 証明書は別々に設定することができます。

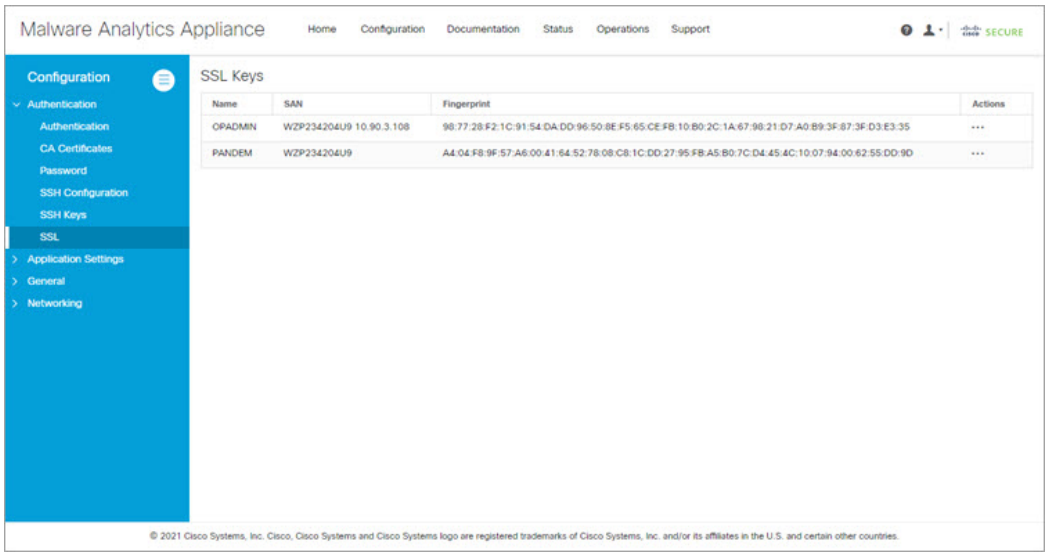
（注） Cisco Secure Malware Analytics アプライアンスが Cisco Secure Endpoint プライベートクラウドを信頼できるようにするアウトバウンド SSL 接続については、CA 証明書を参照してください。

手順

ステップ 1 [構成（Configuration）] タブをクリックします。

ステップ 2 サイド ナビゲーションで **[認証（Authentication）]** を展開し、 **[SSL]** を選択して **[SSLキー（SSL Keys）]** ページを開きます。

図 *35 : [SSL* キー（*SSL Keys***）*]* ページ**



この例では、Admin インターフェイス用の「**OpAdmin**」クリーン インターフェイス用の「**Pandem**」という 2 つの SSL 証明書を取り上げます。

ステップ 3 ホスト名が SSL で使用されている SAN（サブジェクト代替名）と一致していることを確認します。ホスト名は、Cisco Secure Malware Analytics アプライアンスの SSL 証明書で使用される SAN と一致している必要

があります。一致しない場合は、SSL 証明書を再生成できます。「SSL 証明書の再生成」を参照してください。

SSL 証明書の置き換え

通常、SSL 証明書は、証明書が期限切れになった、ホスト名が変更された、または他のシスコデバイスやサービスとの統合をサポートするためなど、さまざまな理由からいずれかの時点で置き換える必要があります。

Cisco ESA、WSA およびその他の CSA シスコ統合デバイスでは、共通名が Cisco Secure Malware Analytics アプライアンスのホスト名と一致するコモン ネームの SSL 証明書が必要な場合があります。デフォルトの SSL 証明書を、同じホスト名を使用して Cisco Secure Malware Analytics アプライアンスにアクセスする、新たに生成された証明書に置き換える必要があります。

Cisco Secure Malware Analytics アプライアンスを Cisco Secure Endpoint プライベートクラウドと統合して、その配置更新サービスを使用する場合は、Cisco Secure Malware Analytics アプライアンスが接続を信頼できるように、Secure Endpoint プライベート クラウド SSL 証明書をインストールする必要があります。

Cisco Cisco Secure Malware Analytics アプライアンスで SSL 証明書を交換するには、複数の方法があります。

- SAN に現在のホスト名を使用する SSL 証明書を再生成します。
- SSL 証明書のダウンロード
- これは商用の SSL や企業向けの SSL の場合もあれば、OpenSSL を使用して作成したものである場合もあります。
- OpenSSL を使用した SSL 証明書の作成

SSL 証明書の再生成

ホスト名が証明書の SAN と一致しない場合は、**[SSL キー（SSL Keys）]** ページで SSL 証明書を再生成できます。

手順

ステップ 1 [構成（Configuration）] タブをクリックします。

ステップ 2 サイド ナビゲーションで **[認証（Authentication）]** を展開し、 **[SSL]** を選択して **[SSLキー（SSL Keys）]** ページを開きます。

ステップ 3 **[アクション（Actions）]** 列で、（**...**）メニューをクリックして、新しい証明書を必要とするインターフェイスのための **[再生成（Regenerate）]** をクリックします。

証明書の SAN フィールドでアプライアンスの現在のホスト名を使用する新しい自己署名 SSL 証明書が Secure Malware Analytics アプライアンス上で生成されます。再生成された証明書（.certファイル）をダウンロードして、統合するアプライアンスにインストールできるようになりました。

SSL 証明書のダウンロード

Cisco Secure Malware Analytics で生成された SSL 証明書（キーはダウンロードできません）はダウンロードできます。ダウンロードした証明書は、クラスタを設定するときに使用できます。また、統合デバイスにインストールして、Cisco Secure Malware Analytics アプライアンスからの接続を信頼できるようにすることもできます。（この手順のためには .cert ファイルのみが必要です。）

手順

ステップ 1 [構成（Configuration）] タブをクリックします。

ステップ 2 サイドナビゲーションで **[認証（Authentication）]** を展開し、 **[SSL]** を選択して **[SSLキー（SSL Keys）]** ページを開きます。

ステップ 3 **[アクション（Actions）]**（**[...]**）メニューから、適切なインターフェイスの **[ダウンロード（Download）]** を選択します。SSL 証明書がダウンロードされます。

SSL 証明書のアップロード

組織で商用または企業向けの SSL 証明書をすでに運用している場合は、その証明書を使用して Cisco Secure Malware Analytics アプライアンス用の新しい SSL 証明書を生成し、統合先のデバイスに対して CA 証明書を使用することができます。

手順

ステップ 1 [構成（Configuration）] タブをクリックします。

ステップ 2 サイドナビゲーションで **[認証（Authentication）]** を展開し、 **[SSL]** を選択して **[SSLキー（SSL Keys）]** ページを開きます。

ステップ 3 **[アクション（Actions）]** 列で、**(...)** メニューをクリックして、適切なインターフェイスの **[アップロード（Upload）]** をクリックします。[**SSL 証明書のアップロード（Upload SSL Certificate）**] ページが開きます。

ステップ 4 **[証明書（Certificate）]** および **[秘密キー（Private Keys）]** フィールドに入力し、 **[証明書の追加（Add Certificate）]**をクリックします。

OpenSSL を使用した SSL 証明書の作成

OpenSSL は、OpenSSL 証明書、キー、その他のファイルを作成および管理するための標準的なオープンソース SSL ツールです。オンプレミスの SSL 証明書インフラストラクチャが設置されていない場合、OpenSSL を使用して SSL 証明書を手動で生成し、Cisco Secure Malware Analytics アプライアンスにアップロードすることができます（「SSL 証明書のアップロード」を参照）。.

（注） OpenSSL は Cisco 製品ではないため、テクニカル サポートは提供されません。OpenSSL の使用方法の詳細については、Web を検索することをお勧めします。シスコは、SSL 証明書を生成するための SSL ライブラリ *Cisco SSL* を提供しています。

手順

ステップ 1 次のコマンドを実行して、新しい自己署名 SSL 証明書を生成します。

（注）
次の例では、より新しい SAN（サブジェクト代替名）ではなく、CN（共通名）を使用しています。

```
openssl req -x509 -days 3650 -newkey rsa:4096 -keyout tgapp.key -nodes -out
tgapp.cert -subj "/C=US/ST=New York/L=Brooklyn/O=Acme Co/CN=tgapp.acmeco.com"
```

openssl：OpenSSL

req：X.509 証明書署名要求（CSR）管理の使用を指定します。X.509 は、キーおよび証明書の管理に SSL と TLS が使用する公開キーインフラストラクチャの標準規格です。次の例では、このパラメータを使用して、新しい X.509 証明書を作成します。

-x509：証明書署名要求を生成せずに、自己署名証明書を作成するように req パラメータ X.509 を変更します。

-days 3650：このオプションは、証明書が有効と見なされる期間を設定します。この例では、10 年間に設定されています。

-newkey rsa: 4096：新しい証明書と新しいキーを同時に生成するように指定します。必要なキーが事前に作成されなかったため、証明書を使用して作成する必要があります。パラメータ「**rsa:4096**」は、4096 ビット長の RSA キーを作成することを示します。

-keyout：このパラメータは、作成中の秘密キーファイルが OpenSSl によって保存される場所を示します。

-nodes：このパラメータは、パスフレーズを使用して証明書を保護するためのオプションを OpenSSL がスキップする必要があることを示します。サーバーの起動時に、アプライアンスは、ユーザーの介入なしでファイルを読み取ることができる必要があります。パスフレーズで保護されている証明書の場合、サーバーの再起動のたびにユーザーがパスフレーズを入力する必要があります。

-out：このパラメータは、作成中の証明書が OpenSSL によって保存される場所を示します。

-subj（例）：

- **C=US**：国
- **ST=New York**：州
- **L=Brooklyn**：場所
- **O=Acme Co**：所有者の名前
- **CN=tgapp.acmeco.com**：Cisco Secure Malware Analytics アプライアンスの FQDN（完全修飾ドメイン名）を入力します。この名前には、Cisco Secure Malware Analytics アプライアンスのホスト名（この例では **tgapp**）と、関連するドメイン名（この例では **acmeco.com**）が含まれます。

  重要
  Cisco Secure Malware Analytics アプライアンスのクリーンインターフェイスの FQDN と一致するように、少なくとも共通名を変更する必要があります。

ステップ 2 新しい SSL 証明書が生成されたら、**[SSL キー（SSL Keys）]** ページから Cisco Secure Malware Analytics アプライアンスに証明書をアップロードします（「SSL 証明書のアップロード」を参照）。これらのデバイスで統合されない場合、E メール セキュリティ アプライアンスまたは Web セキュリティアプライアンスに証明書（**.cert** ファイルのみ）をアップロードする必要もあります。

アプリケーション設定

Cisco Secure Malware Analytics アプライアンスのアプリケーション設定は、このパネルで行います。

統合

TitaniumCloud、Umbrella（OpenDNS）、VirusTotal といった複数のサードパーティ検出およびエンリッチメント サービスとの統合を **[Integration]** ページを使用してアプライアンスで構成できます。

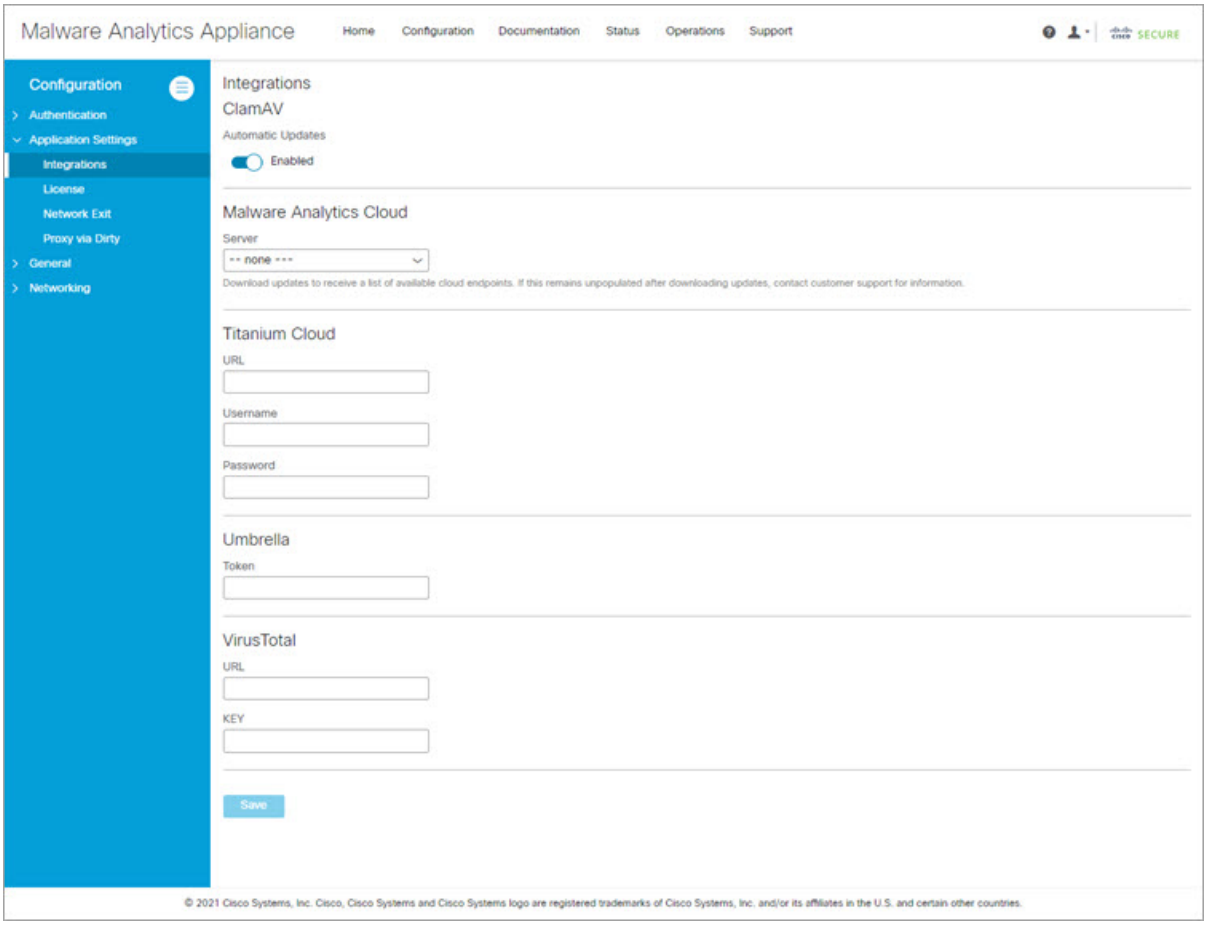
クラウド検索フェデレーション機能 (v2.8 以降で利用可能) では、クラウド エンドポイントが以下のように構成されている場合、Secure Malware Analytics ポータル UI で、Secure Malware Analytics クラウド インスタンスに対して検索クエリを再実行するオプションがユーザーに提供されます。

（注） Umbrella (OpenDNS) が構成されない場合、分析レポート（Cloud UI）のドメイン エンティティ ページの **whois** 情報は表示されません。

手順

ステップ 1 **[構成（Configuration）]** > **[アプリケーション設定（Application Settings）]** > **[統合（Integrations）]**に移動します。

図 *36 :* 統合構成ページ



[統合（Integrations）] 画面が表示されます。

ステップ 2 [Malware Analytics Cloud] で、**[US Cloud]** または **[EU Cloud]**を選択します。選択したクラウドサービス（**US クラウド** または **EU クラウド**）のアカウントがあることを確認します。

（注）
デフォルトでは、マルウェア分析クラウドのリージョンは **[なし（None）]**に設定されています。クラウドベースの分析を有効にするには、最初に更新の確認を実行する必要があります。更新チェックの実行に関する情報は、「更新 （138 ページ）」を参照してください。

Cisco Secure Malware Analytics（SMA）から、Cisco Secure Malware Analytics クラウドに接続するためのプロビジョニングが提供されます。クラウド接続を介して、**サンプル配置ルックアップ**を活用できます。この機能により、SMA アプライアンスは Secure Malware Analytics クラウド内の中央データベースを検索できま

す。このデータベースには、SMAユーザーコミュニティ全体によって送信された、以前に分析されたファイル（サンプル）に関する情報が保存されます。

図 37 : サンプルダッシュボード：*Cisco Secure Malware Analytics* クラウドのリンク

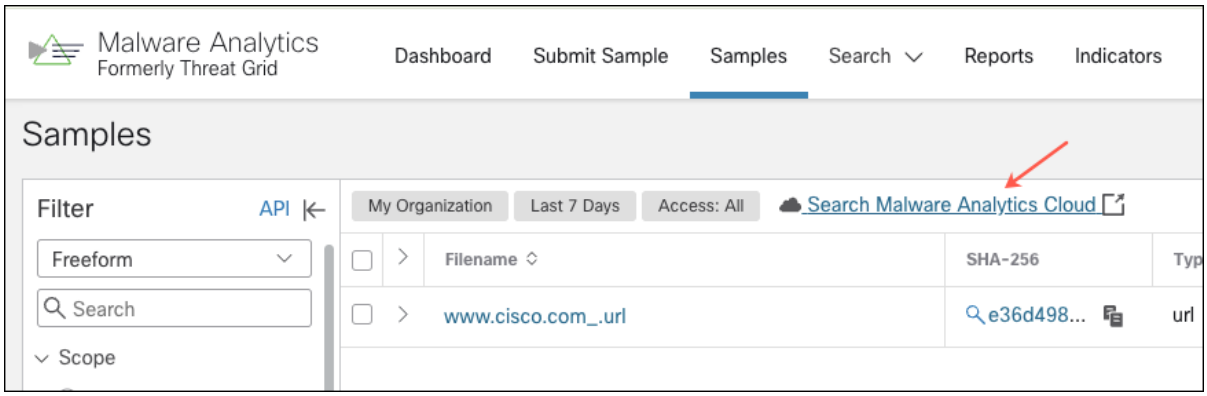
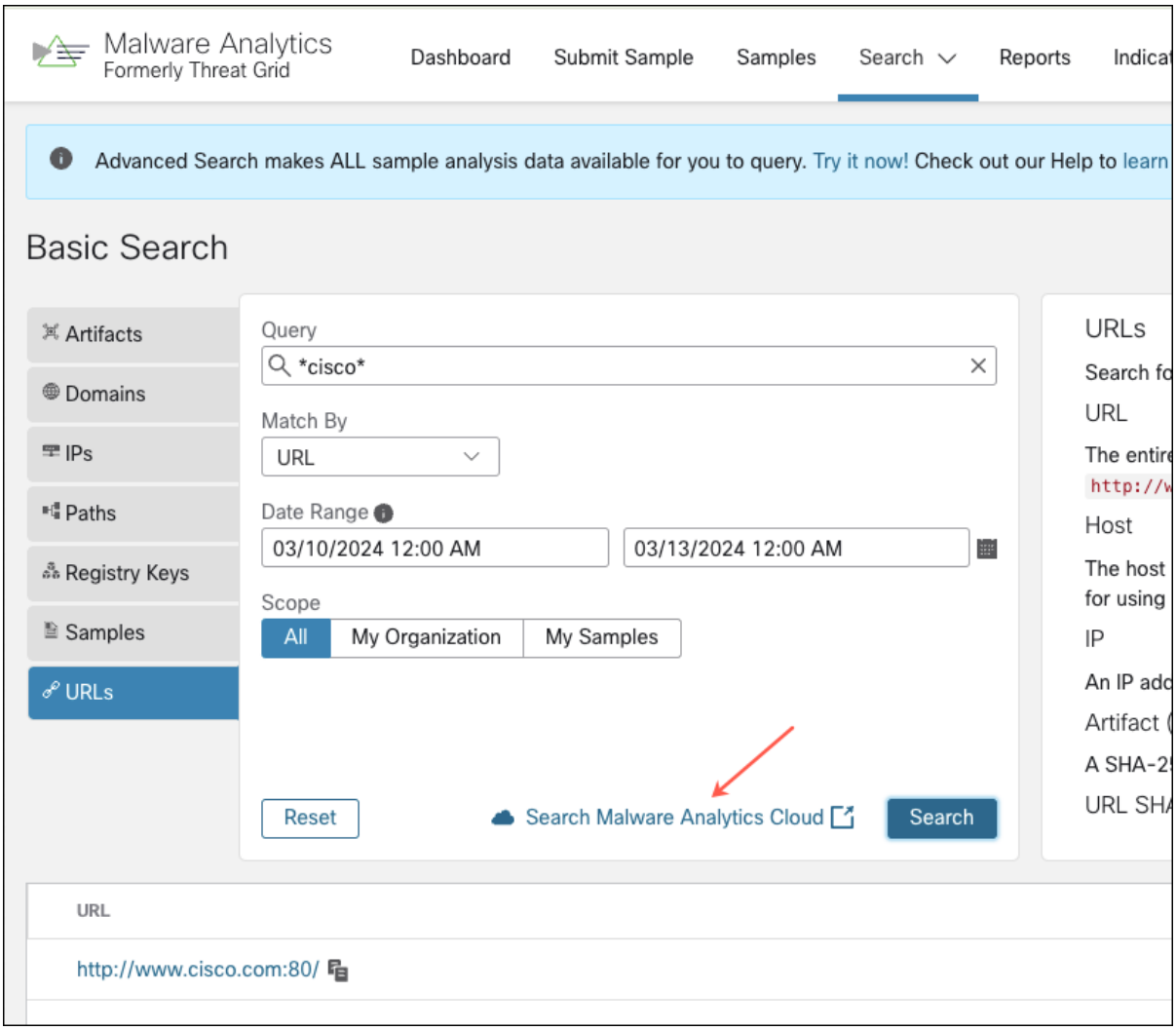


図 *38* : 基本検索 : ***Cisco Secure Malware Analytics*** クラウドのリンク



（注）
Cisco Secure Malware Analytics アプライアンスではデータセキュリティが優先されます。マルウェア分析クラウドでサンプル処理ルックアップを実行しても、実際のサンプルファイル自体はクラウドにアップロードまたは転送され **ません** 。

この機能では、次の 2 つのインテリジェンス ソースでの検索を有効にすることで、アプライアンスの機能を拡張します。

- **ローカル インテリジェンス ストア** : このアプライアンス上のデータベースには、以前に分析されたファイルに関する情報が保存されます。
- **クラウド インテリジェンス ストア** : Cisco Secure Malware Analytics クラウド内のこの集中型リポジトリでは、SMA ユーザーベース全体からの脅威データが集約されます。

ステップ 3 各統合に必要なログイン情報を入力します。

（注）
ClamAV シグネチャは、毎日自動的に更新でき、デフォルトで有効になっています。マルウェア分析で ClamAV シグニチャを有効にすると、ClamAV のウイルスシグニチャのデータベースを使用して、既知のマルウェアを検出できるようになります。 **[ClamAV]** セクションで **[自動更新（Automatic Updates）]** 設定を無効にできます。

チタン クラウド（ReversingLabs TitaniumCloud™）

さまざまなクラウドサービスの統合マルウェア分析プラットフォームを使用し、60 億ファイルを超えるグローバル提供およびマルウェア データベースを利用してファイルを特定することにより、検出、分析、および対応の効率性を向上させます。

統合を構成するには、 次のものが必要です。

1. **URL**： TitaniumCloud の URL。
2. **[ユーザー名（Username）]**： TitaniumCloud アカウントのユーザー名。
3. **[パスワード（Password）]**： TitaniumCloud アカウントのパスワード。

Umbrella（Cisco - 以前の名前は OpenDNS）

Cisco Umbrella を既存のセキュリティ インフラストラクチャに統合することで、DNS 層で悪意のあるドメインと IP をブロックし、リアルタイムの脅威インテリジェンスを提供し、他のセキュリティ ツールと統合することで、マルウェア検出を改善できます。これにより、ユーザーが悪意のあるリンクをクリックしたり、感染した添付ファイルを開いたりした場合でも、マルウェアがコマンドアンドコントロール サーバーに接続したり、悪意のあるペイロードをダウンロードしたりすることを防ぐことができます。Cisco Umbrella との統合を設定するには、Cisco Umbrella ポータルで[管理]に移動して **トークン**を取得します。

（注）
Cisco Umbrella 統合には、階層 2 または階層 3 の Investigate ライセンスが必要です。

VirusTotal

VirusTotalは、疑わしいファイルと URL を分析し、ウイルス、ワーム、トロイの木馬、およびあらゆる種類のマルウェアを検出する無料のサービスです。セキュリティ運用と簡単に統合できます。VirusTotal をセキュリティ インフラストラクチャに統合することで、大規模で包括的なマルウェア データベースへのアクセス、新しいマルウェアや出現するマルウェアを検出する機能、および疑わしい URL やファイルをサンドボックスで分析する機能により、マルウェア検出を改善できます。VirusTotal 統合を使用する前に、プラグインをアクティブ化し、適切な API キーとともにアクティブ化されたインスタンスの URL を提供する必要があります。

ステップ 4 [保存（Save）] をクリックします。

ライセンス

新しいアプライアンスを購入すると、ライセンスが生成され、 **[構成（Configuration）] > [ライセンス（License）]** ページの **[サーバーからライセンスを取得（Retrieve License From Server）]** ボタンが有効になります。ただし、それが機能しない場合、または特殊なケース（ライセンス

がカスタムのワンオフであるなど）がある場合、ライセンスはパスワードとともに暗号化されたファイルとして直接提供されます。

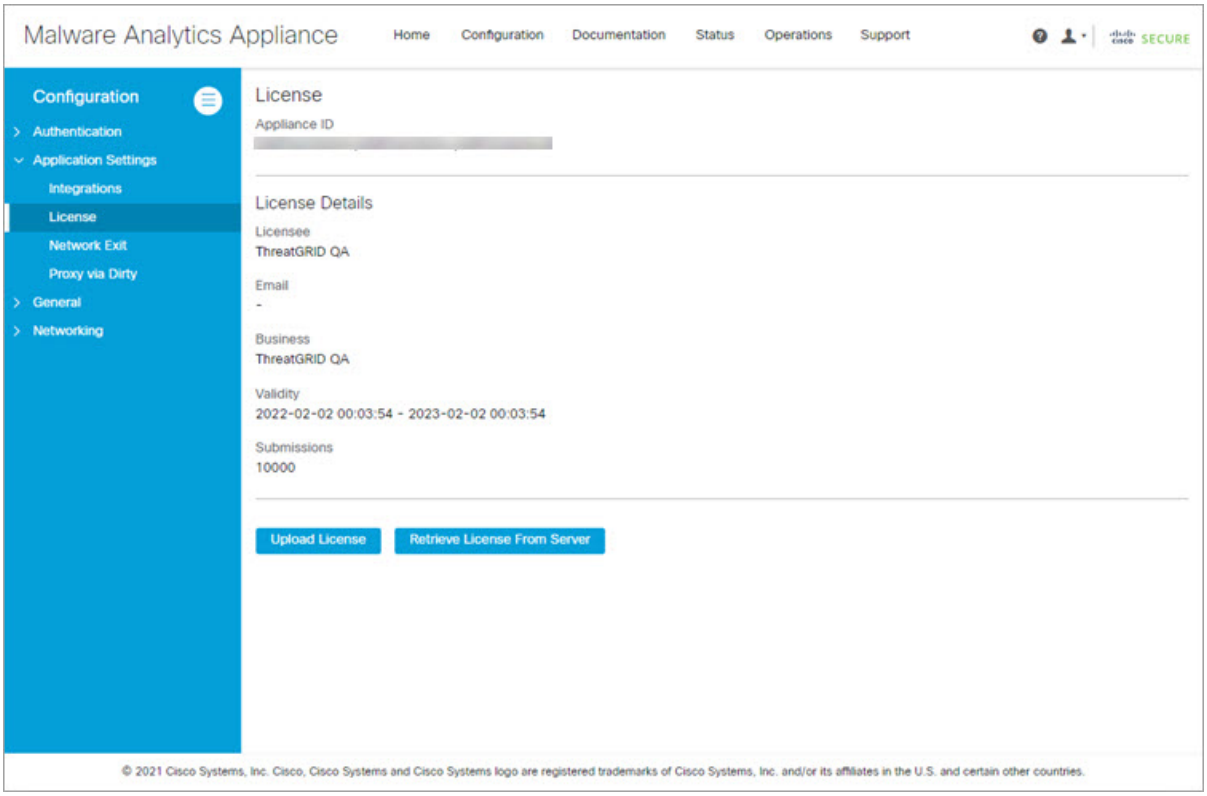
[ライセンス（License）] ページを使用して、ライセンス情報を表示または更新できます。

手順

ステップ 1 [構成（Configuration）] タブをクリックします。

ステップ 2 サイドナビゲーションで**[アプリケーション設定（Application Settings）]** を展開し、**[ライセンス（License）]** を選択して **[ライセンス（License）]** ページを開きます。

図 *39 : [ライセンス（License）]* ページ

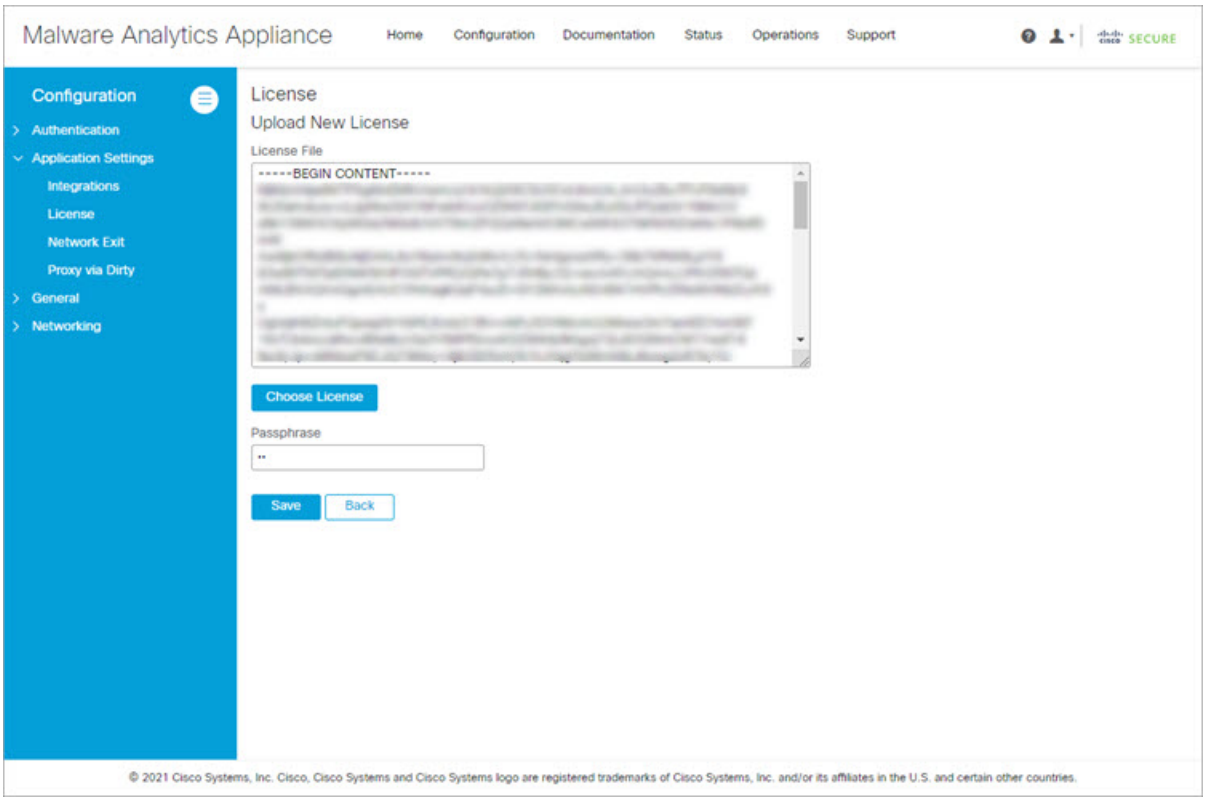


ステップ 3 ライセンスをアップロードするか、サーバーから取得します。通常、エアギャップアプライアンスのライセンスをアップロードする必要があります。

ライセンスのアップロード方法：

a) **[ライセンスのアップロード（Upload License）]** をクリックして、**[新しいライセンスのアップロード（Upload New License）]** ページを開きます。

図 *40* : 'ライセンスのアップロード'



b) **[ライセンスの選択（Choose License）]** をクリックして **ファイルマネージャ** を開き、Cisco Secure Malware Analytics から受け取ったライセンスファイル（ファイルの拡張子が .lic）を選択して、**[開く（Open）]** をクリックします。

ライセンスの内容が **[ライセンス ファイル（License File）]** フィールドに追加されます。

c) Cisco Secure Malware Analytics が（.lic ファイルで）提供したパスワードを **[パスフレーズ（Passphrase）]** フィールドに入力し、**[保存（Save）]** をクリックします。

再構成が必要であることを示すアラートが表示されます。「構成変更の適用」を参照してください。

サーバーからのライセンスの取得方法：

a) **[サーバーからライセンスを取得（Retrieve License From Server）]** をクリックして、ライセンスを取得して追加します。

b) [保存（Save）] をクリックします。

再構成が必要であることを示すアラートが表示されます。「構成変更の適用」を参照してください。

Network Exit

地理的な場所は、マルウェア分析において重要な問題になることがよくあります。マルウェアのいくつかの種類は、地理的な場所によって異なる方法で動作しますが、その他の種類は特定の領域をターゲットにする可能性があります。VPN の概念と同様に、**Network Exits** モード（v2.4.3 以降で利用可能）により、サンプル分析中に生成されるすべての発信ネットワークがその場所で終了したように表示されます。構成ファイルが自動的に配布されるため、サポートスタッフが手動でインストールまたは更新する必要はありません。

（注） **tg-tunnel and v2.4.3**： 以前に tg-tunnel を使用していた場合は、v2.4.3 をインストールする前に、Network Exit に必要な特定の IP アドレスとポートへのアウトバウンドトラフィックを許可する必要があります。それ以外の場合は、リモート終了の使用を有効にする前に、該当するトラフィックのみを許可する必要があります。必要な IP アドレスとポートはときどき変更されます。最新のリストについては、「Threat Grid に必要な IP およびポート」 を参照してください。

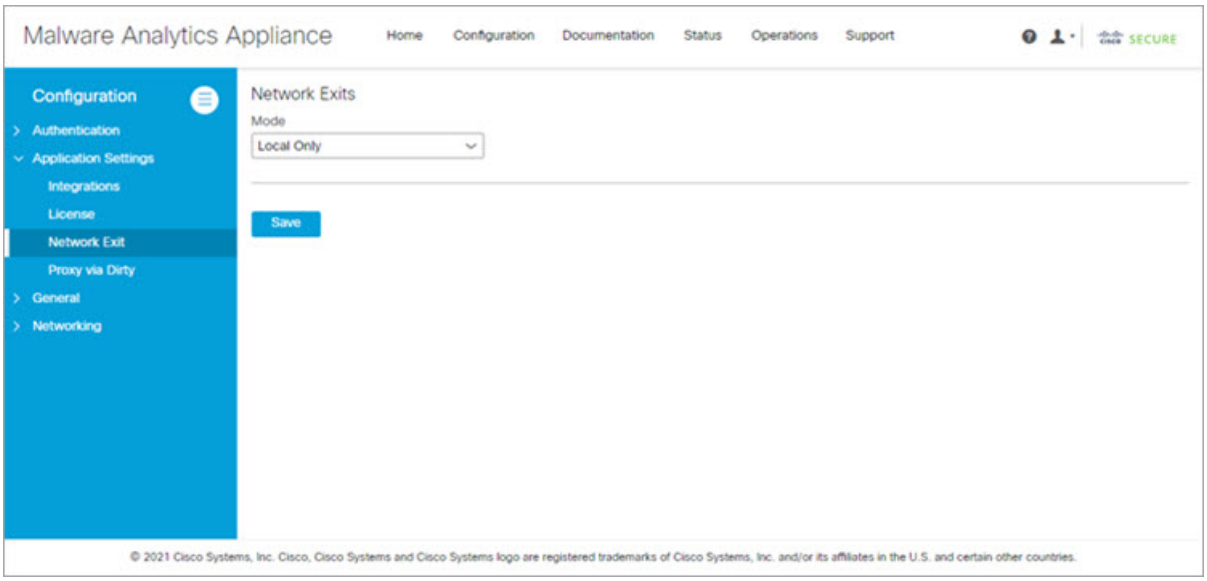
手順

ステップ 1 [構成（Configuration）] タブをクリックします。

ステップ 2 サイドナビゲーションで **[アプリケーション設定（Application Settings）]** を展開し、 **[Network Exit]** を選択して **[Network Exits]** の構成ページを開きます。

このページの設定によって、分析用のサンプルの送信時に Cisco Secure Malware Analytics ポータルで使用可能な **[Network Exit]** オプションが決まります。

図 *41 : Network Exits* 構成



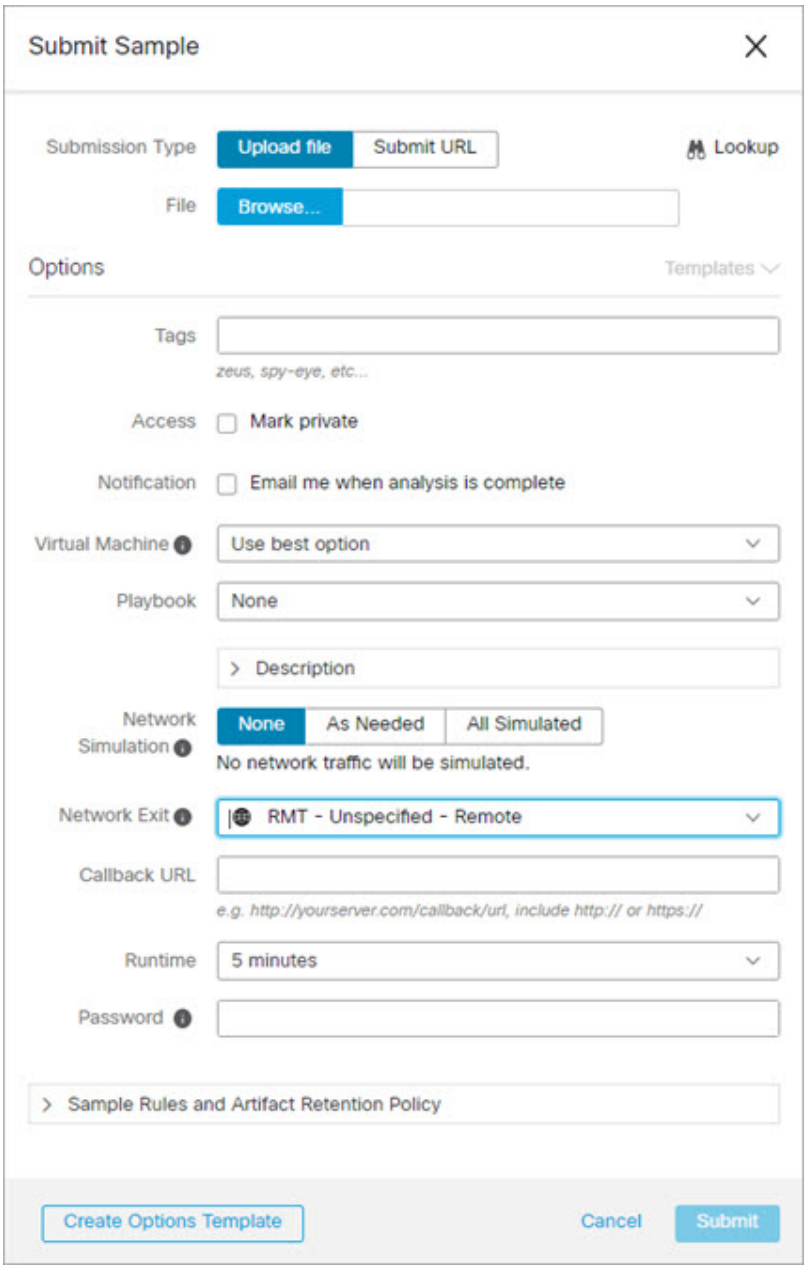
ステップ 3 [モード（Mode）] ドロップダウンリストから、**[ローカルのみ（Local Only）]**、**[リモートのみ（Remote Only）]**、**[ローカルとリモートの両方（Both Local and Remote）]**、または **[シミュレーションのみ（Simulation Only）]**を選択します。

[ローカルのみ（Local Only）] または **[リモートのみ（Remote Only）]**を選択した場合、アプリケーションでユーザーはそれらのオプションのみを使用できます。 **[ローカルとリモートの両方（Both Local and Remote）]**を選択すると、ユーザーは両方のオプションを使用できます。

[シミュレーションのみ（Simulated Only）] を選択した場合、API ユーザーと UI ユーザーは、仮想マシンからローカル Cisco Secure Malware Analytics アプライアンス外の接続先にネットワークトラフィックを送信するオプションを選択できません。

プライベートネットワークへのアクセスは、DNS ルックアップやネットワーク終了が目的であっても許可されません。すべてのマルウェアトラフィックは、設定済みのダーティ DNS サーバーを使用して、ダーティインターフェイスから発信されます。

図 *42* : サンプルの送信



（注）
分析中にネットワーク接続をシミュレートする必要が生じることがあります。ネットワーク シミュレーションは、それ以外の方法では（または他の理由で）使用できない可能性があるマルウェアサンプルにネットワークリソースを提示する方法をアナリストに提供します。たとえば、アップストリームサーバーにアクセスできない場合、サーバーがダウンしている場合、DNS レコードが失われた場合、またはサンプルの実行率と判定率を向上させるためにアウトバウンド接続に対する他の制限が適用されている場合に、ネットワーク接続をシミュレートするネットワーク シミュレーション オプションを選択できます。

さらに、ネットワーク シミュレーションは、エアギャップアプライアンスへの接続方法を少なくともいくつか提供し、それらのアプライアンスに対するサンプルの実行率を改善することができます。

サンプル分析の**ネットワーク シミュレーション**オプションは、Cisco Secure Malware Analytics Appliance v2.7.1 以降で使用できます。詳細については、Cisco Secure Malware Analytics ポータル UI のオンラインヘルプトピックを参照してください。

プロキシの更新

SOCK5 は、プロキシ サーバーを介してクライアントとサーバー間でネットワーク パケットを交換するインターネットプロトコルです。アプライアンスのダーティインターフェイスが更新サーバーに到達できない場合。SOCKS5 プロキシは、更新をダウンロードするように構成されている。

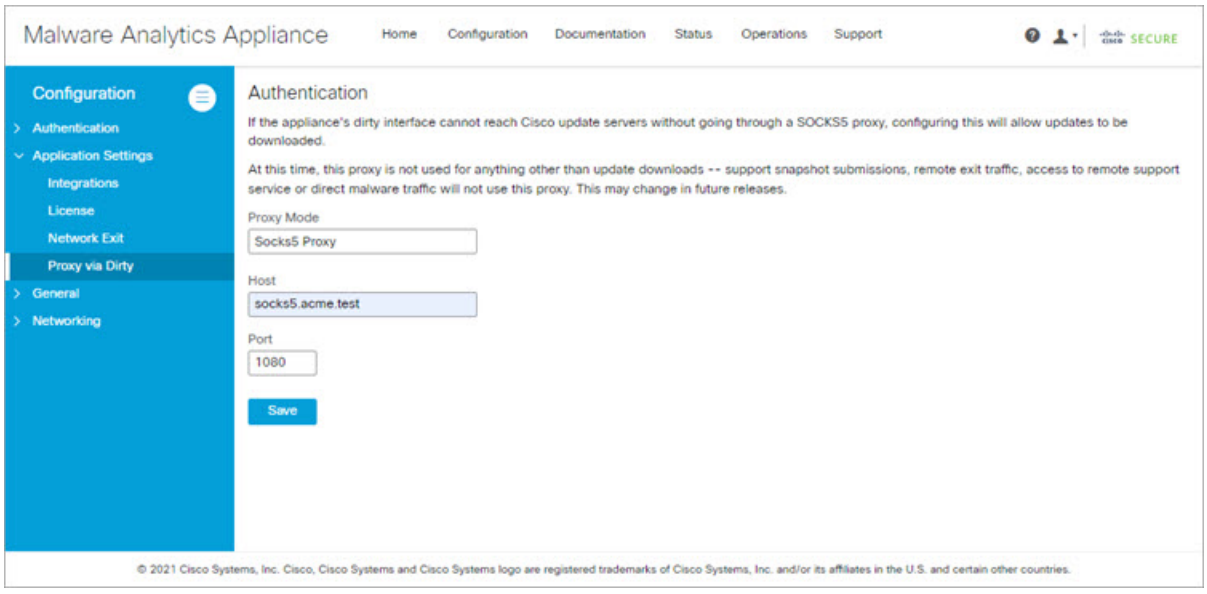
手順

ステップ 1 [構成（Configuration）] タブをクリックします。

ステップ 2 サイド ナビゲーションで **[アプリケーション設定（Application Settings）]** を展開し、**ダーティ経由でプロキシ**を選択して、 **[認証（Authentication）]** 構成ページを開きます。

このページの設定によって、更新プログラムのダウンロードに使用される **[更新プロキシ（Updates proxy）]** のオプションが決まります。

図 *43 :* プロキシ設定の更新



ステップ 3 **[プロキシ モード（Proxy Mode）]** ドロップダウン リストから、**[Socks5 プロキシ（Socks5 Proxy）]**を選択します。

ステップ 4 **[ホスト（Host）]** フィールドにホストを入力します。

ステップ 5 **[ポート（Port）]** フィールドにポートを入力します。

全般

Cisco Secure Malware Analytics アプライアンスの一般的な構成設定は、[一般（General）] サイドナビゲーションの下にあります。

コンテンツの更新

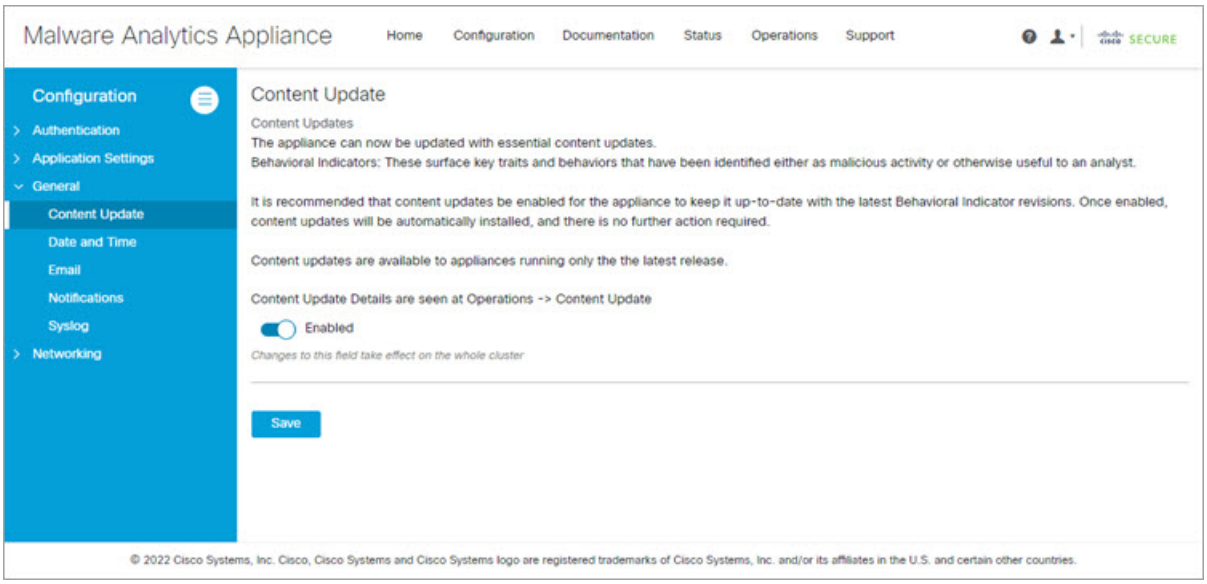
[コンテンツの更新（Content Update）]により、アプライアンスはアプライアンスの更新中に最新の動作インジケータを自動的に受信できます。BI を自動的に受信するには、[コンテンツ更新（Content Update）] スイッチを **[有効（Enabled）] の** 位置に切り替える必要があります。[コンテンツの更新（Content Update）] を有効にするには、次の手順を実行します。

手順

ステップ 1 [構成（Configuration）] タブをクリックします。

ステップ 2 サイドナビゲーションで **[一般（General）]** を展開し、**[コンテンツの更新（Content Update）]** を選択して **[コンテンツの更新（Content Update）]** ページを開きます。

図 *44* : コンテンツの更新



（注）
[Content Update] を有効にすると、クラスタ内のすべてのアプライアンスが更新されます。

ステップ 3 スイッチを **[無効（Disabled）]** から **[有効（Enabled）]** に切り替えます。

（注）
有効にすると、夜間のアプライアンス更新チェック中にコンテンツ更新がダウンロードされ、適用されます。

ステップ 4 [保存（Save）] をクリックします。

日時

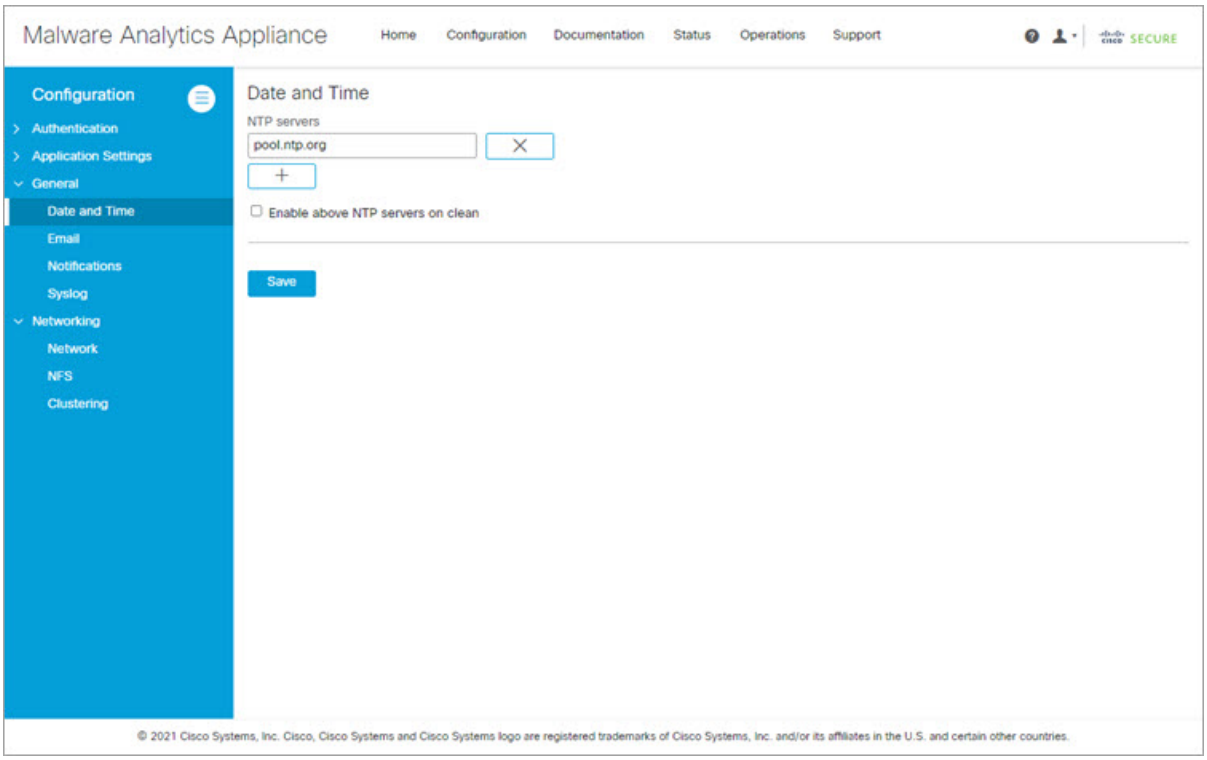
Cisco Secure Malware Analytics アプライアンスを最初に設定する際に、Network Time Protocol（NTP）サーバーを指定して日付と時刻を設定します。 **[日付と時間（Date and Time）]** ページを使用して、NTP サーバを追加または削除できます。

手順

ステップ 1 [構成（Configuration）] タブをクリックします。

ステップ 2 サイドナビゲーションで **[一般（General）]** を展開し、 **[日付と時間（Date and Time）]** を選択して **[日付と時間（Date and Time）]** ページを開きます。

図 *45* : 日時



ステップ 3 NTP サーバーの追加または削除

- **[+]**アイコンをクリックして別のフィールドを追加し、NTP サーバ名または IP アドレスを入力します。必要に応じて繰り返します。
- サーバを削除するには、 **[x]** アイコンをクリックします。

ステップ 4 [保存（Save）] をクリックします。

E メール

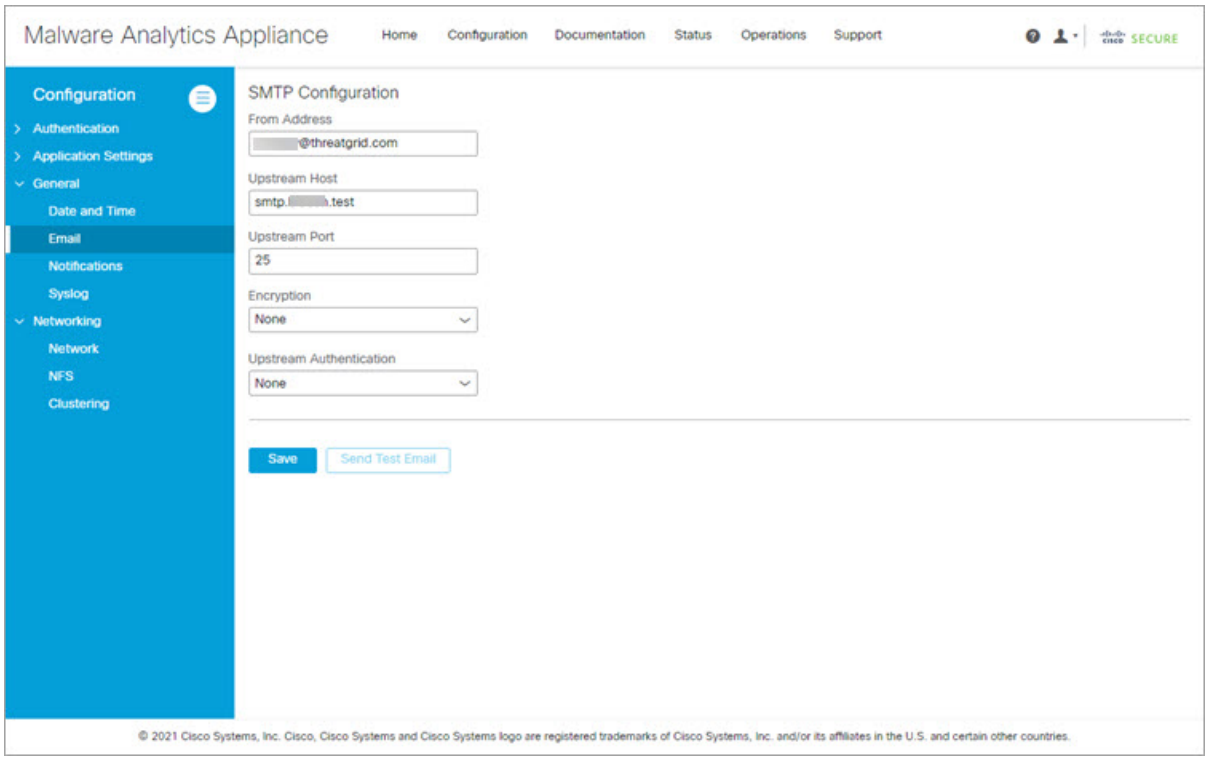
Cisco Secure Malware Analytics アプライアンスの初期セットアップ時に、電子メールの設定を行います。これらの設定は、**[電子メール（Email）]** ページで変更できます。

手順

ステップ 1 [構成（Configuration）] タブをクリックします。

ステップ 2 サイドナビゲーションで **[一般（General）]** を展開し、 **[電子メール（Email）]** を選択して **[SMTPの構成（SMTP Configuration）]** ページを開きます。

図 *46 : SMTP*の設定



ステップ 3 変更を加えて、**[保存（Save）]**をクリックします。

再構成が必要であることを示すアラートが表示されます。「構成変更の適用」を参照してください。

ステップ 4 **[テスト メールの送信（Send Test Email）]** をクリックして、SMTP 構成をテストします。

通知

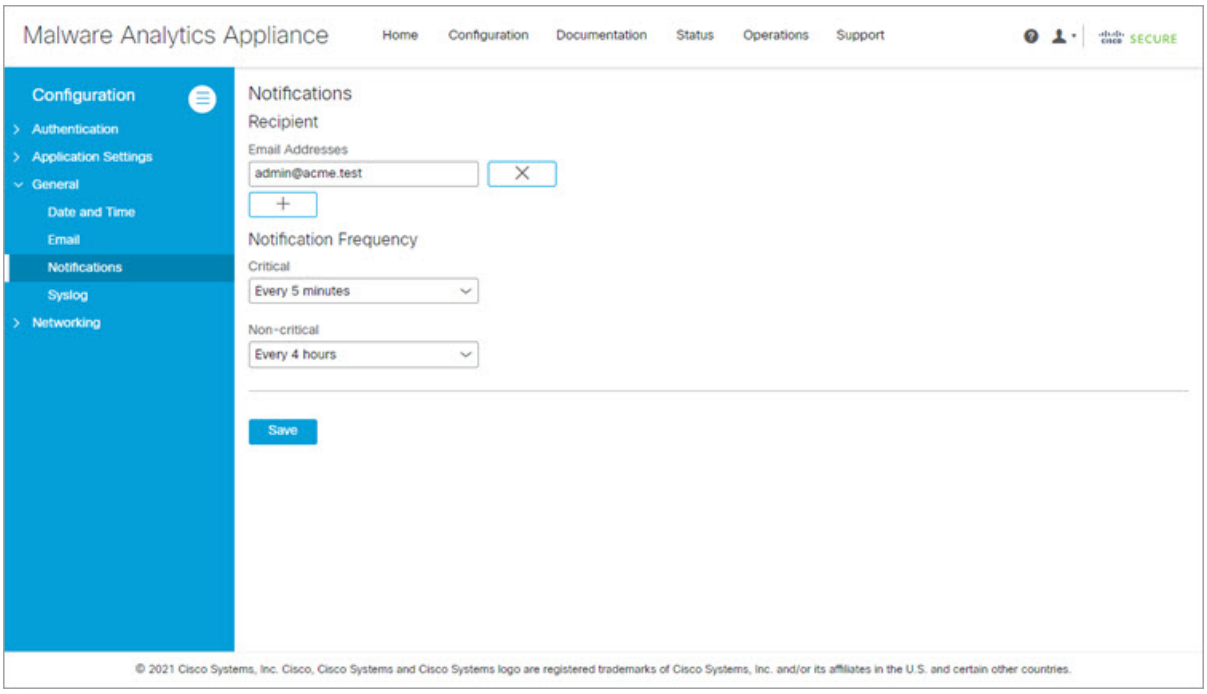
Cisco Secure Malware Analytics アプライアンスの初期設定時に、電子メールで通知を受信するように構成します。 **[通知（Notifications）]** ページを使用して、受信者を追加または削除したり、通知頻度を変更したりできます。

手順

ステップ 1 [構成（Configuration）] タブをクリックします。

ステップ 2 サイド ナビゲーションで **[一般（General）]** を展開し、 **[通知（Notifications）]** を選択して **[通知（Notifications）]** ページを開きます。

図 *47 :* 通知



ステップ 3 [受信者（Recipients）] で、少なくとも 1 人の通知受信者の [電子メールアドレス（Email Address）] を入力します。複数の電子メールアドレスを追加する必要がある場合は、[+] アイコンをクリックして別のフィールドを追加します。必要に応じて繰り返します。

ステップ 4 [通知頻度（Notification Frequency）] で、ドロップダウンリストから [重大（Critical）] および [非重大（Non-critical）] の設定を選択します。

ステップ 5 [保存（Save）] をクリックします。

Syslog

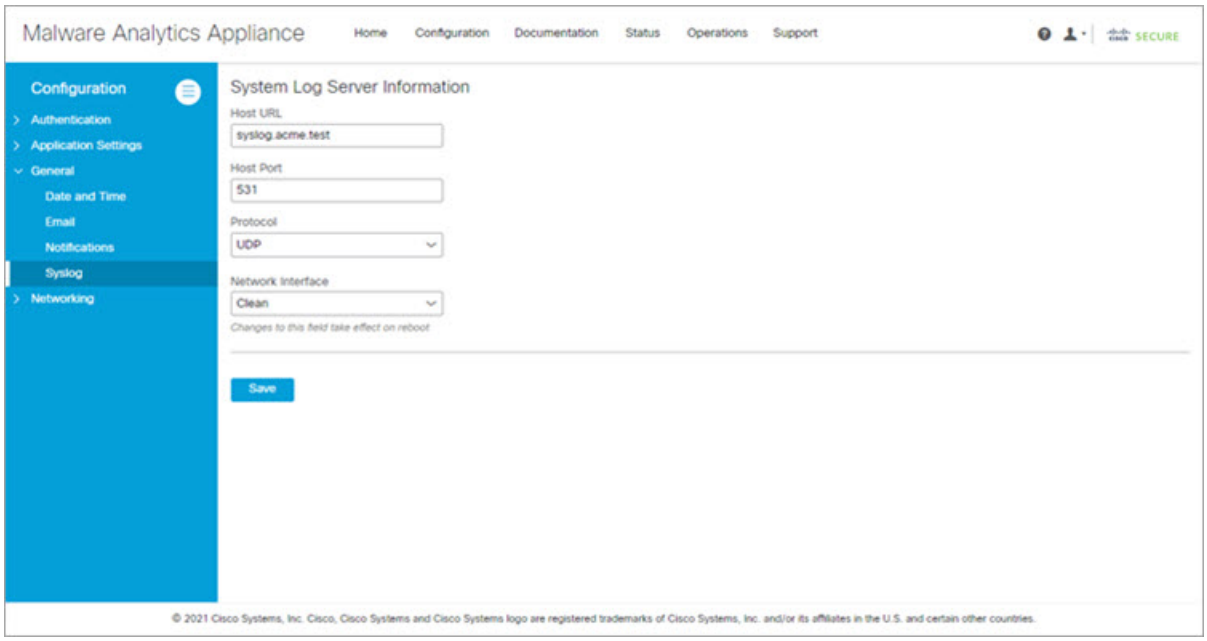
[システムログサーバー情報（System Log Server Information）] ページは、Syslog メッセージおよび Thread Grid 通知を受信するためのシステムログサーバーの設定に使用されます。

手順

ステップ 1 [構成（Configuration）] タブをクリックします。

ステップ 2 サイドナビゲーションで **[一般（General）]** を展開し、 **[Syslog]** を選択して **[システムログ（System Log）]** **[サーバー情報（Server Information）]** ページを開きます。

図 *48 :* システムログサーバー情報



ステップ 3 このページのフィールドに入力します。

- **ホスト URL**（**Host URL**）：システムログサーバのホスト名または URL を入力します。
- **ホスト ポート**：サーバのポート番号を入力します。
- **プロトコル**：ドロップダウン リストから **TCP** または **UDP** を選択します。

ステップ 4 [保存（Save）] をクリックします。

ネットワーキング

Cisco Secure Malware Analytics アプライアンスのネットワーク構成設定は、[ネットワーキング（Networking）] サイドのナビゲーションの下にあります。

ネットワーク

初期設定に DHCP を使用した後、3 つのネットワークすべてに関して、IP 割り当てを DHCP から固定的な静的 IP アドレスに調整する必要がある場合は、次の手順を実行します。

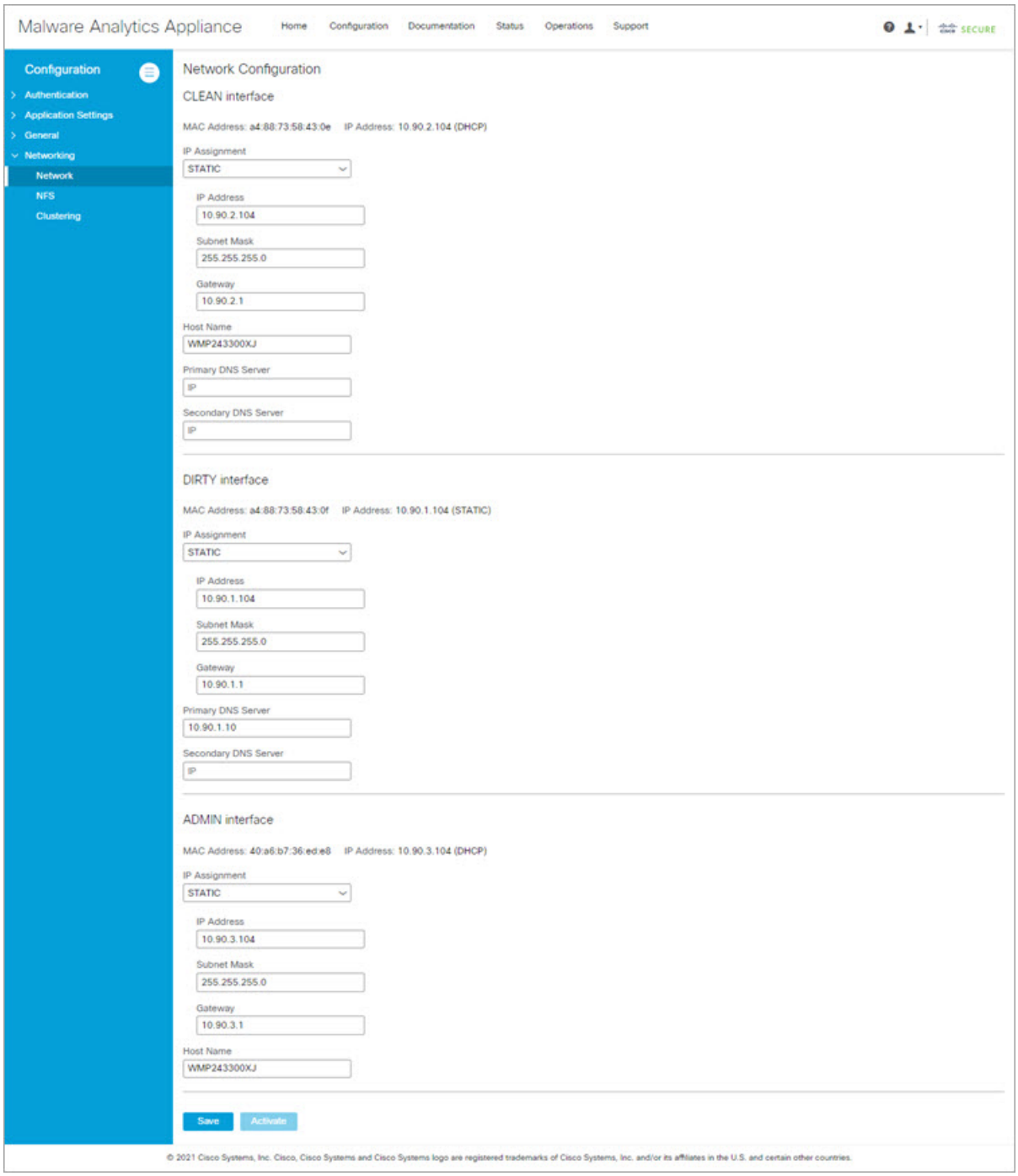
（注） Admin UI はゲートウェイ エントリを検証しません。誤ったゲートウェイを入力して保存すると、Admin UI にアクセスできなくなります。ネットワーク設定を管理インターフェイスで実行した場合は、コンソールを使用してネットワーク設定を修正する必要があります。Admin がまだ有効であればい、Admin UI でそれを修正して、再起動できます。

手順

ステップ 1 [構成（Configuration）] タブをクリックします。

ステップ 2 サイドナビゲーションで **[ネットワーキング（Networking）]** を展開し、 **[ネットワーク（Network）]** を選択して **[ネットワーク構成（Network Configuration）]** ページを開きます。

図 *49* : ネットワーク設定



ステップ 3 次のフィールドに入力します。

（注）
Admin ネットワークの設定は、Secure Malware Analytics アプライアンスの初期セットアップおよび構成中に、Admin TUI を使用して行われています。

- [**IP 割り当て**] - 3 つすべてのインターフェイスのドロップダウンリスト（Clean、Dirty、および Admin）から、**Static** を選択します。
- [**IP Address**]：クリーンまたはダーティ ネットワーク インターフェイスの静的 IP アドレスを入力します。
- [**サブネットマスクとゲートウェイ（Subnet Mask and Gateway**）] - ネットワーク インターフェイスのタイプに応じて入力されます。
- **[ホスト名（Host Name** ）]：サーバーのホスト名を入力します。
- [**プライマリ DNS サーバー（Primary DNS Server**）**]**：プライマリ DNS サーバー アドレスを入力します。
- [**セカンダリ DNS サーバー（Secondary DNS Server**）**]**：セカンダリ DNS サーバーの情報を入力します。

（注）
ADMIN Interface： 正常を 通過するように *Admin* からトラフィックを再ルーティングするには、**[IP 割り当て（IP Assignment**）**]** で **[DISABLED]** を選択します。

ステップ 4 **[保存（Save**）**]** をクリックしてネットワーク設定を保存してから、**[アクティブ化（Activate**）**]**をクリックします。

再設定が必要であることを示すメッセージが表示されます（ 構成変更の適用」を参照）。

DNS の設定

デフォルトで、DNS はダーティ インターフェイスを使用します。Secure Endpoint プライベートクラウドなど、統合先のアプライアンスまたはサービスのホスト名がダーティインターフェイスで解決できない（統合にクリーンインターフェイスが使用されるため）場合は、クリーンインターフェイスを使用する別の DNS サーバーを Admin UI で構成できます。

手順

ステップ 1 [構成（Configuration）] タブをクリックします。
ステップ 2 サイドナビゲーションで **[ネットワーキング（Networking**）**]** を展開し、**[ネットワーク（Network**）**]** を選択して **[ネットワーク構成（Network Configuration**）**]** ページを開きます。
ステップ 3 ダーティネットワークとクリーンネットワークの [**DNS**] フィールドに入力します。
ステップ 4 [保存（Save）] をクリックします。

NFS

Cisco Secure Malware Analytics アプライアンス（v2.2.4 以降）は、NFS 対応ストレージへの暗号化されたバックアップ、NFS 対応ストレージからのデータの初期化、さらに、データベースを空の状態にリセットして前述のバックアップのロードを可能にする機能をサポートしています。

（注） リセットは、アプライアンスのワイププロセスとは異なっており、アプライアンスが情報漏えいなしで顧客構内に出荷されるようにするために使用され、バックアップ準備のためにも使用されます。その目的に適したワイププロセスは、リカバリブートローダーにすでに存在していますが、バックアップを復元するためのシステムの準備には適していません。

コンテンツは、サードパーティ製オープンソース製品である gocryptfs を使用して暗号化されます。

（注） パフォーマンス上の理由から、ファイル名の暗号化は無効になっています。Cisco Secure Malware Analytics 内のサンプルとその他のコンテンツは、どのような状況でも元の名前では保存されないため、顧客の所有データが漏洩することはありません。

ご使用の前に、ドキュメントをよくお読みいただくことを強くお勧めします。バックアップの機能に関する詳細ドキュメントを入手できます。使用する前によくお読みいただくことを強くお勧めします。追加の技術情報と手順については、『Cisco *Secure Malware Analytics Appliance Backup Notes and FAQ*』を参照してください。

NFS 要件

NFS バックアップストレージへの暗号化されたバックアップを実現するには、次の NFS 要件を満たす必要があります。

- Cisco Secure Malware Analytics アプライアンスの管理インターフェイスからアクセス可能な、TCP を介した NFSv4 プロトコルを実行する必要があります。
- ルートユーザー（UID 0）のみがマウントできます。マウント時に UID 0 が許可されていることを確認してください。Windows NFS 管理者には、その場所に書き込みできる UID 0 のユーザーが必要です。

（注） Linux サーバーの場合、 *root_squash* はデフォルトで使用可能なので重要ではありません。ただし、厳密な環境では、 *no_root_squash* を追加できません。

- 構成されているディレクトリは、**nfsnobody**（UID 65534）で書き込み可能である必要があります。

- **nfsnobody** による書き込みへのファイルの公開は安全です。**nfsnobody** または **nfsnobody** として実行されている Cisco Secure Malware Analytics アプライアンスでの唯一のプロセスは、データの暗号化に関するプロセスです。プレーンテキストデータは、最小権限の原則に基づいて、さまざまなサブツリーの個別のユーザーアカウントで公開されます。アプライアンス上の PostgreSQL サービスは、Elasticsearch データやフリーザにアクセスできません。Elasticsearch サービスは、PostgreSQL やフリーザデータにアクセスできません。
- **nfsnobody** アカウントを使用すると、設定が簡素化され、カスタマーサイトごとに **idmap.conf** を構築する必要がなくなり、ローカルとリモートのアカウント名が一緒にマッピングされます。

- NFSv4 サーバーは、10 GB 管理インターフェイス経由でアクセス可能である必要があります。
- 十分なストレージが使用可能である必要があります（「バックアップストレージの要件」を参照）。
- システムは次のパラメータを使用します。`rw`、 `sync`、 `nfsvers=4`、 `nofail`

（注） 競合するパラメータを入力しないでください。これらと競合するパラメータを手動で入力することがサポートされないのは明白で、未定義の動作が発生する可能性があります。

- 無効な NFS 設定（または誤って設定された NFS サーバーへのサービスをポイントした設定）の結果として、多くの場合、設定を適用するプロセスに失敗します。Admin UI でのこの設定を修正して再適用すると成功します。

バックアップ ストレージ要件

バックアップストアに合計で 5.6 TB を超えるストレージは必要ありません。バックアップ ストアは、次のコンポーネントで構成されています。

- **オブジェクトストア**：通常、使用されるストレージの大部分を占めています。バックアップストアの一括コンポーネントでのデータ保持は、使用中の Cisco Secure Malware Analytics アプライアンスリリース向けに文書化されたものと同じポリシーと制限に従っており、このコンポーネントの最大ストレージ使用量は 4.1 TB です。「Cisco Secure Malware Analytics アプライアンスデータの保持に関する注意事項」を参照してください。
- **PostgreSQL データベースストア**：PostgreSQL ストアの 2 つの完全バックアップと、保持されている完全バックアップのうち一番古いものから再生するのに十分な一連の WAL ログが含まれます。合計 500 GB 未満にする必要があります。
- **Elasticsearch スナップショットストア**：合計 1 TB 未満にする必要があります。

バックアップで予想される成果

次のバックアップで予想される成果を考慮する必要があります。

- **バックアップに含まれる**：Cisco Secure Malware Analytics アプライアンスのバックアップ プロセスの最初のリリースには、次の顧客独自の一括データが含まれます。
  - Samples
  - 分析結果、アーティファクト、フラグ付き
  - アプリケーション層の（Admin UI ではない）組織およびユーザー アカウントのデータ。
  - データベース（ユーザーおよび組織を含む）
  - Cisco Secure Malware Analytics ポータル UI 内で設定を行います。
- **バックアップに含まれない** - 次のものは、Secure Malware Analytics アプライアンス バックアップ プロセスに含まれていません。
  - [System logs]
  - 以前にダウンロードおよびインストールした更新
  - SSL キーと CA 証明書を含む、アプライアンス OpAdmin インターフェイスでの構成
- **その他の期待**：バックアッププロセスに関するその他の考慮事項は次のとおりです。
  - PostgreSQL ベースバックアップは 24 時間サイクルで実行されます。データベースのバックアップの復元はできません。少なくとも 1 回正常に完了するまで警告が表示されます。
  - Elasticsearch バックアップは 5 分ごとに段階的に行われます。
  - Freezer バックアップは、進行中のバックアップから失われたオブジェクトを処理するために、24 時間ごとに後続のジョブを使用して継続的に実行されます。
  - 新しいキーを生成すると、新しい独立したバックアップストアが作成されます。オリジナルのように、この新しいストアは、24 時間サイクルのベース バックアップが行われるまで有効になりません。

バックアップ データの保持

バックアップの際、次のようにデータが保持されます。

- **PostgreSQL**：最後の 2 つの正常なバックアップと、それらのバックアップ以降のすべての WAL セグメントが保持されます。
- **Elasticsearch**：最新の 5 分ごとのスナップショット 2 回分が保持されます。
- **一括ストレージ** - 単一の Secure Malware Analytics アプライアンス向けに使用され文書化されるものと同じ保持ポリシーが、共有ストアに対して使用されます。

長期間にわたって履歴データを保持する場合は、ファイルシステムレイヤまたはブロックレイヤのスナップショットをサポートする NFS サーバーを使用することを強くお勧めします。

データベースのベースバックアップは、新しいベースバックアップが正常に作成されるまで保持されます。

（注） バルクストレージでの障害発生後のリセット時に使用するため、仮想マシンイメージのバックアップコピーが RAID-1 ストレージアレイ上に作成されます。初期の Cisco Secure Malware Analytics アプライアンスモデル（UCS C220-M3 プラットフォームをベースとする）は、後のモデルよりもストレージが小さく、Secure Malware Analytics アプライアンス v2.9 のインストール後に、他のユニットが使用できる空き容量が、RAID-1 ファイルシステムのディスク容量の 25 % 未満になる可能性が高くなります。その場合、サービス通知がトリガーされます。

後のモデルのハードウェアで、v2.9 リリースのインストール後に、RAID-1 アレイの空きストレージが 25 % 未満になる場合、これは正常な状態ではないため、カスタマーサポートに問い合わせる必要があります。

保持期限の厳密な適用

TGSH（v2.6 以降）の **strict_retention** オプションを使用すると、分析済みのアーティファクトを 15 日間を超えて保存しないことにより、保持期間の制限を厳密に適用することができます。このオプションを有効にすると、最初の夜間プルーニングの際に、15 日間を超えて保存されているファイルが削除されます。

（注） 15 日の期間を設定または変更することはできません。

アーティファクトとは、サンプル自体と、サンプルから生成されたその他のものを意味します。アーティファクトには分析レポートの HTML が含まれていません。分析レポートの HTML は、別途記載されているとおり、最初から制限の対象となります。アーティファクトには、データベースエントリや検索インデックスも含まれません。

strict_retention オプションは、デフォルトでは無効（false）になっています。15 日後のアーティファクトのハードプルーニングを有効にするには、**TGSH** でこのオプションを true に設定します。

configure set strict_retention true

バックアップ頻度

データのバックアップ頻度は次のとおりです。

- サンプル、アーティファクト、レポートのバルクストレージの場合、コンテンツは継続的にバックアップされます。さらに、パスが実行されると、24 時間サイクルで不足しているコンテンツが検索されて転送されます。

- PostgreSQL データベースの場合、ベースバックアップが 24 時間サイクルで作成され、その後は、新たに書き込まれたデータベースコンテンツが 16 MB のしきい値に達するごとに、または 5 分ごとに、増分コンテンツが継続的に追加されます。
- Elasticsearch データベースの場合、コンテンツはバックアップ ストアに 5 分間サイクルで段階的に追加されます。

バックアップの頻度を制御または調整することはできません。頻度を変更すると、ストレージ使用率、復元の処理時間、パフォーマンスのオーバーヘッドに関する想定が無効になるためです。

バックアップ関連のサービス通知

バックアッププロセス中に、次のサービス通知が表示される場合があります。

- 「**ネットワークストレージがマウントされていません（Network storage not mounted）**」：バックエンドとして使用されているネットワーク ファイル システムが完全に動作していることを確認して、Admin UIOpAdmin で設定を再適用するか、アプライアンスを再起動します。
- 「**Network storage not working（ネットワークストレージが動作していません）**」：バックエンドとして使用されているネットワーク ファイル システムが完全に動作していることを確認します。システムが NFS サーバーの問題の修正から 15 分以内に回復しない場合は、アプライアンスを再起動してください。
- 「**Backup file system access failure（バックアップ ファイル システムのアクセスに失敗しました）**」：カスタマーサポートまでお問い合わせください。
- **PostgreSQL のバックアップが見つかりません**：これは、バックアップ ストアが設定された時間内のポイントと（自動的に24時間サイクルで実行される）最初のベースバックアップが行われる時間内のポイント間で正常な状態です。これが完了するまで、バックアップ完了とは見なされず、復元することはできません。このメッセージが 48 時間を超えて続く場合または続く場合に限り、カスタマー サポートに連絡してください。
- 「**Newest PostgreSQL base backup more than two days old（最新の PostgreSQL ベース バックアップは 3 日以上前です）**」：システムが PostgreSQL の新しいベースバックアップの生成に成功していないことを示します。修正されない場合、（古くなりつつあるバックアップ ポイントから復元するために必要な書き込みの完全なチェーンを保持するための）バックアップ ストアでの使用が制限されなくなり、行われる復元に必要な処理時間が許容できる長さを超えます。サポートにお問い合わせください。
- 「**Backup Creation Messages（バックアップ作成メッセージ）**」：バックアップの開始またはトリガーの際に検出されたエラーを反映しています。
- **非アクティブの ES バックアップ（作成）**：Elasticsearch が開始して、バックアップ ストアが使用不可能であることを示します。この状態は、アプライアンスを再起動するか、（NFS と暗号化サービスが機能している場合）**TGSH** にログインして `restart elasticsearch.service` コマンドを実行することで改善できます。

- バックアップのメンテナンス メッセージ：**以前に作成されたバックアップのステータスを確認するときにこれらのリフレクト エラーが検出されました。**
- 「**ES Backup (Maintenance) snapshot (...) status FAILED（ES バックアップ（メンテナンス）スナップショット（...）のステータスが [FAILED] になっています）**」：Elasticsearch データベースのバックアップの最近の更新で、インデックスが正常に書き込まれなかったことを示します。NFS サーバーが機能していて空き領域があることを確認します。問題を特定できず、解決しない場合は、カスタマー サポートにお問い合わせください。
- 「**ES Backup (Maintenance) snapshot (...) status INCOMPATIBLE（ES バックアップ（メンテナンス）スナップショット（...）のステータスが [INCOMPATIBLE] になっています）**」：アプライアンスのアップグレードで新しいバージョンの Elasticsearch がインストールされた直後にのみ発生します。バックアップストアがアップグレードされて、新しいリリースとの互換性を持つようになるまで表示されます。この状態の間に障害が発生した場合、互換性のないバックアップからの復元には、カスタマーサービスの支援が必要になることがあります。
- 「**ES Backup (Maintenance) snapshot (...) status PARTIAL（ES バックアップ（メンテナンス）スナップショット（...）のステータスが [PARTIAL] になっています）**」：本文に次の 2 つのメッセージのうちのいずれかが含まれています。「No prior successful backups seen, so retaining（以前に成功したバックアップが見つからないため、そのまま保持します）」（バックアップは存在するものの部分的でしかない場合）。または「Prior successful backups exist, so removing（以前に成功したバックアップが存在するため、削除します）」（後で再試行するために部分的なバックアップを破棄しようとしている場合）。
- 「**ES Backup (Maintenance) - Backup required (...) ms（ES バックアップ（メンテナンス）：バックアップに（...）分間かかります）**」：バックアップに 60 秒を超える時間が必要な場合に発生します。これは必ずしもエラーとは限りません。Elasticsearch では定期的なメンテナンスを実行し、これがアイドル状態のシステムにも重要な書き込み負荷を発生させることがあります。ただし、これが負荷が少ない期間で一貫して発生する場合は、ストレージ パフォーマンスを調査するか、サポートが必要な場合はカスタマー サービスに連絡してください。
- 「**ES Backup (Maintenance) - Unable to query Elasticsearch snapshot status（ES バックアップ（メンテナンス）：Elasticsearch スナップショット ステータスのクエリを実行できませんでした）**」：Elasticsearch に接続できませんでした。この障害は、バックアップの作成が正常に開始された後に発生します。一般に、他のアプライアンスの障害と同時に発生するため、それらの問題の修復に重点を置く必要があります。アプライアンスが他の点では完全に機能しているときにこのエラーが発生し、自分では解決できない場合は、カスタマー サポートに問い合わせてください。

[Appliance Backup]

Cisco Secure Malware Analytics アプライアンスのバックアップを実行するには、次の手順を実行します。

手順

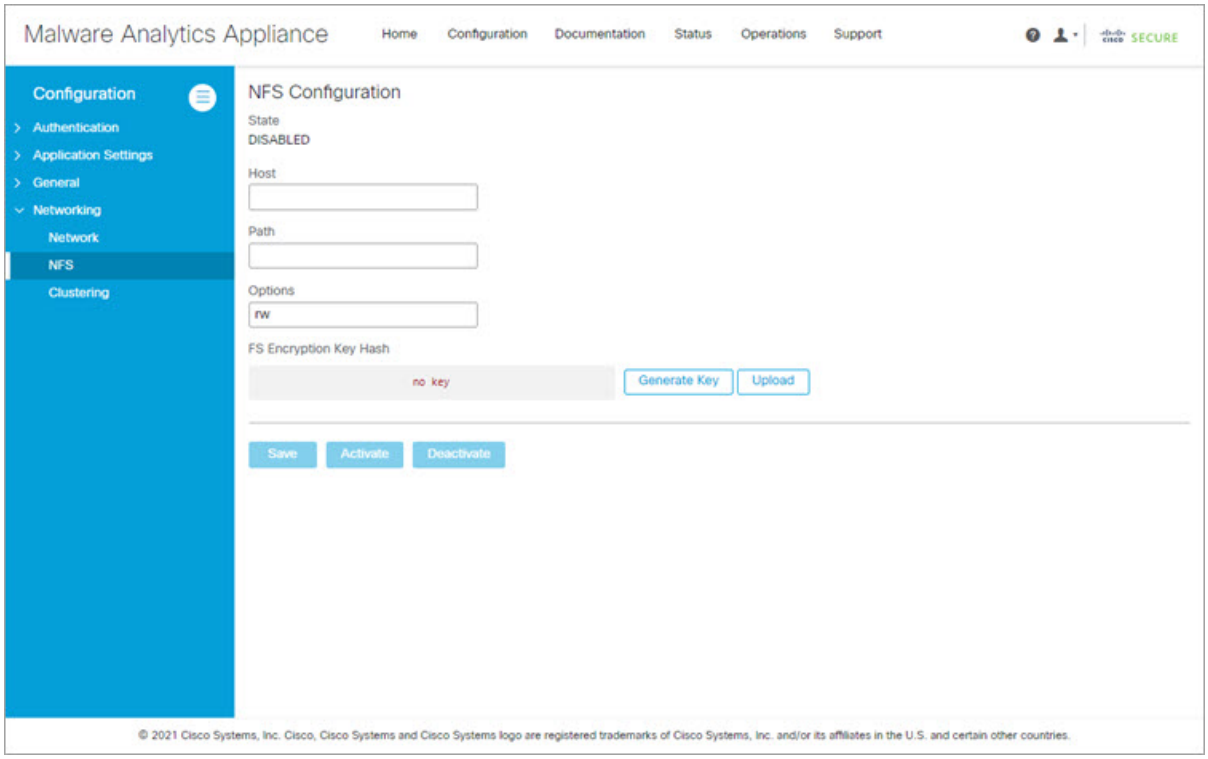
ステップ 1 「NFS」に従って、バックアップのターゲットディレクトリを作成します。

ステップ 2 [構成（Configuration）] タブをクリックします。

ステップ 3 サイドナビゲーションで **[Networking]** を展開し、 **[NFS]** を選択して **[NFSの構成（NFS Configuration）]** ページを開きます。

（注）
アプライアンスの初期設定時に NFS の設定を完了し、暗号キーを持っている場合は、ステップ 3 からステップ 5 までを省略できます。そうでない場合は、バックアップデータを復元するために暗号化キーを取得する必要があります。

図 *50 : NFS* の設定



ステップ 4 次の情報を入力します。

- [**Host**]：NFSv4 ホストサーバー。IP アドレスを使用することをお勧めします。
- [**Path**]：NFS ホストサーバー上のロケーションへの絶対パス。ここにファイルが保存されます。
- **オプション**：このサーバーで NFSv4 に対する標準 Linux のデフォルト値を変更する必要がある場合に使用される NFS マウントオプション。デフォルトは **rw** です。

- [FS暗号化キーハッシュ（FS Encryption Key Hash）] : [キーの生成（Generate Key）] をクリックして、新しい暗号化キーを生成します。後でバックアップを復元するには、このキーが必要になります。（その時点で、[アップロード（Upload）] をクリックして、バックアップに必要なキーをアップロードします。）

ステップ 5 [保存（Save）] をクリックします。ページが更新され、**FS 暗号化パスワードキー ID** が表示されます。

このページを最初に設定するときに、暗号化キーを**削除**または**ダウンロード**するオプションが表示されます。NFS が有効になっているがキーが作成されていない場合は、[Upload] オプションが表示されます。キーを作成すると、[Upload] ボタンが [Download] ボタンに変わります。（キーを削除すると、[ダウンロード（Download）] ボタンが再び [アップロード（Upload）] になります。）

（注）
キーがバックアップを作成するために使用されたキーと正確に一致する場合、アップロードが設定されたパスのディレクトリ名と一致した後、**キー ID** が管理 UI に表示されます。暗号キーを使用せずにバックアップを復元することはできません。

ステップ 6 キーをアクティブ化するには、**[アクティブ化（Activate）]** をクリックします。

重要
ユーザーが暗号キーをバックアップして安全に保管する責任。 Cisco Secure Malware Analytics はコピーを保持しません。このキーを使用せずにバックアップを完了することはできません。

ステップ 7 「バックアップ復元ターゲットとしての Cisco Secure Malware Analytics アプライアンスのリセット」の説明に従って、アプライアンスをバックアップ復元ターゲットとしてリセットします。

ステップ 8 バックアップコンテンツの復元 （110 ページ） の説明に従って、バックアップデータを復元します。

バックアップ復元ターゲットとしての Cisco Secure Malware Analytics アプライアンスのリセット

アプライアンスを復元ターゲットとして使用する前に、事前設定された状態にする必要があります。アプライアンスは、この状態で出荷されます。ただし、設定した後に事前設定された状態に戻すには、明示的な管理操作が必要になります。

注意 このプロセスを実行すると、お客様が所有するデータが破棄されます。タスクを実行する前にすべてのマニュアルを読み、慎重に作業を続行してください。.

（注） リセットは、リカバリ モードで使用できるセキュア ワイプと同じものではありません。DLP 再イメージ化センターに発送する前に、お客様が所有するデータをアプライアンスから完全に削除するのに適しているのは、リカバリモードでのセキュア ワイプのみです。ただし、リカバリモードでのセキュアワイプは、リセットに代わるものではありません。セキュアワイプでは、再イメージ化されるまで使用できなくなるアプライアンスが処理され、リセットでは、アプライアンスがバックアップを復元する準備が行われます。

データのリセット

データリセットプロセスが Cisco Secure Malware Analytics アプライアンス v2.7 以降で更新され、さらに包括的になりました。すべての顧客関連データの確実な破壊を保証するため、（リカバリ ブートローダー メニューの）ワイププロセスは依然として必要ですが、リセットプロセスにより、オペレーティングシステムのログや、そのまま残されていた他の状態がクリアされるようになりました。

Cisco Secure Malware Analytics アプライアンスが正常にリセットされると、新しいランダム生成のパスワードがコンソールに表示されるようになりました（新規インストール時の動作と同じです）。この改善されたプロセスでは、複数回再起動するようになっています。また、リカバリモードからの起動が可能になりました（以前のプロセスでは、通常の操作で起動した場合にのみ正常に起動することが可能でした）。

Cisco Secure Malware Analytics アプライアンス（v2.7 以降）は、プライマリファイルシステムとして XFS を使用します。Cisco Secure Malware Analytics アプライアンスのデータがリセットされると、データストアは、XFS ファイルシステムに変更されます。これにより、前方互換性が向上し、サービス単位の I/O 使用率のモニタリングに OS レベルのサポートが提供されるようになります。

また、更新されたデータリセットプロセスでは、システム SDD への新規インストールに必要なすべてのコンテンツを格納するのに十分なストレージが必要です。既存のデータは、このコンテンツの存在と有効性が確認された後にのみ削除されます。長期間にわたって使用されているシステム（特に第 1 世代のハードウェア）の場合、すぐに使用できる十分な空き容量がない可能性があります。その場合は、必要に応じてカスタマーサポートの支援を受けることができます。

ターゲットのアプライアンスを事前設定された状態に戻す

メーカーから届いたばかりのシステムで復元するわけではない場合、既存のデータと NFS 関連の設定をシステムから消去することによって、復元のターゲットアプライアンスを事前設定された状態に戻す必要があります。

手順

ステップ 1 Cisco Secure Malware Analytics アプライアンスの TTY または SSH 経由で Admin TUI にアクセスします。

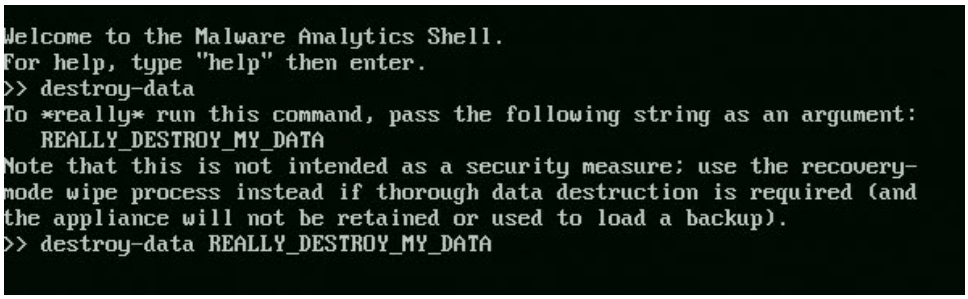
ステップ 2 **[コンソール（Console）]** オプションを選択して、「**tgsh**」と入力します。

（注）
リカバリモードによる「**tgsh**」の入力は、この使用例には適していません。

ステップ 3 **tgsh** プロンプトで、コマンド `destroy-data` を入力します。プロンプトをよく読んで、指示に従ってください。

注意
このコマンドを実行すると、元に戻すことはできません。すべてのデータが破棄されます。

図 *51 : destroy-data REALLY_DESTROY_MY_DATA* コマンドと引数



次のデータが破棄されます。

- Samples
- 分析結果、アーティファクト、フラグ付き
- アプリケーション層の（Admin UI ではない）組織およびユーザー アカウントのデータ。
- データベース（ユーザーおよび組織を含む）
- ネットワーク情報を含むすべてのタイプの構成
- Cisco Secure Malware Analytics ポータル UI 内で設定を行います。
- NFS の設定とログイン情報
- NFS に使用される暗号キーのローカルコピー

ターゲットでないアプライアンスを事前設定された状態に戻す

別のシステムまたはSecure Malware Analyticsアプライアンスが、復元中のバックアップにアクティブに書き込みを行っている場合（実稼働でアクティブに使用されている第2マスターSecure Malware Analyticsアプライアンスが書き込んでいるコンテンツのテスト復元など）、そのSecure Malware Analyticsアプライアンスを事前設定された状態に戻します。

手順

ステップ 1 データストアの一貫した書き込み可能なコピーを生成します。

ステップ 2 テスト復元を実行している Secure Malware Analytics アプライアンスを、継続的に書き込まれているストアではなく、書き込み可能なコピーにポイントします。

Secure Malware Analytics アプライアンスが事前設定された状態の場合は、「バックアップコンテンツの復元」で説明されているとおり、バックアップストアのターゲットとして機能します。

バックアップコンテンツの復元

重要

- 復元プロセスの間、システムをサンプル送信に使用することはできません。
- 特定のアクティブなバックアップストアのデータを使用して一度に実行できるのは、1 台のサーバーのみです。
- バックアップは Admin UI からのみ復元できます。
- 以前に使用したものと同じ NFS ストアと暗号キーを、最初のプロセスと同じプロセスで設定します。以前の NFS ストアと暗号キーを使用して Cisco Secure Malware Analytics アプライアンスを設定すると、復元がトリガーされます。
- プライマリ Cisco Secure Malware Analytics アプライアンスの動作中に別の Cisco Secure Malware Analytics アプライアンスで復元プロセスをテストするには、バックアップストアの一貫したスナップショットのコピーを作成し、（アップロードされた暗号化キーを使用して）新しい Cisco Secure Malware Analytics アプライアンスをポイントします。

バックアップコンテンツを復元するには、次の手順を実行します。

手順

ステップ 1 **[構成（Configuration）]** タブをクリックし、**[NFS]** を選択して **[NFS 構成（NFS Configuration）]** ページを開きます。

ステップ 2 **[Upload]** をクリックして、バックアップが作成されたサーバーの設定時に生成されたバックアップキーを取得します。

このキーがバックアップの作成に使用されたキーと正確に一致する場合、Admin UI ポータルに表示される **キー ID** は、設定されたパス内のディレクトリ名と一致している必要があります。インストールウィザードによってバックアップキーと一致するディレクトリが検索され、そのディレクトリが検出されると、検出された場所へのデータの復元が開始されます。

（注）
経過表示バーは表示されません。データの復元に必要な時間は、バックアップのサイズや他の要因によって異なります。テストによると、1.2 GB の復元は迅速ですが、1.2 TB の復元には 16 時間以上かかります。大規模な復元の場合、インストールがハングしているように見えることがありますが、しばらくお待ちください。Admin UI に復元が成功したとレポートされ、アプライアンスが起動します。

ステップ 3 復元されたデータが元のデータと同じであることを確認します。

クラスタ

クラスタリングは、2 ～ 7 のノードで構成されるクラスタに一緒にいくつかの Cisco Secure Malware Analytics アプライアンスを結合することで、単一のシステムのキャパシティを増やします。またクラスタのサイズに応じて、クラスタ内の 1 つ以上のアプライアンスが障害から回復するのをサポートする点でも役立ちます。クラスタ内の各 Cisco Secure Malware Analytics アプライアンスは、共有ファイルシステムにデータを保存し、クラスタ内の他のノードと同じデータを保持します。

重要 クラスタのインストールまたは再設定について不明な点がありましたら、データの破壊を避けるため、シスコサポートまでお問い合わせください。

機能

Cisco Secure Malware Analytics アプライアンスのクラスタリングは、次の機能を提供します。

- **共有データ**：クラスタ内のすべての Cisco Secure Malware Analytics アプライアンスは、スタンドアロンであるかのように使用できます。それぞれが同じデータにアクセスして表示することができます。
- **サンプル送信処理**：送信されたサンプルは、いずれかのクラスタメンバーで処理され、他のメンバーは分析結果を確認できます。
- **レート制限**：各メンバーの送信レート制限を積算した値がクラスタの制限になります。
- **クラスタサイズ**：推奨されるクラスタのサイズは、3、5、または7 メンバーです。4 および 6 ノードのクラスタはサポートされますが、ノードが 1 つ多いものの機能が低下したクラスタ（1 つ以上のノードが動作していないクラスタ）と同様の可用性になります。
- **タイブレーカー**：クラスタに偶数のノードを含めるように設定すると、タイブレーカーとして指定されたノードは、どのノードがプライマリデータベースを持つかを決定するイベントで二番手に位置付けられます。

  クラスタ内の各ノードにはデータベースが含まれていますが、プライマリノードのデータベースのみが実際に使用されます。プライマリノードがダウンした場合、他のノードがその役割を引き継ぐ必要があります。条件を設定していると、ノードがちょうど半分失敗したとき、ただし、条件が失敗したノード上ではない場合のみ、クラスタがダウンするのを防止できます。

  奇数クラスタには、関連付けられた投票はありません。奇数クラスタでは、（タイブレーカーではない）ノードがクラスタからドロップされた場合にのみ、タイブレーカーロールが関係することになります。その場合、クラスタは偶数クラスタになります。

制限事項

Cisco Secure Malware Analytics アプライアンスのクラスタリングには、次の制限があります。

- 既存のスタンドアロンの Cisco Secure Malware Analytics アプライアンスのクラスタを作成するとき、第1ノード（最初のノード）のみがそのデータを保持できます。クラスタに既存のデータをマージすることは許可されないため、他のノードは手動でリセットする必要があります。

  「バックアップ復元ターゲットとしての Cisco Secure Malware Analytics アプライアンスのリセット」に記載されているとおり、destroy-data コマンドを使用して既存のデータを削除します。

重要 シスコに返却してイメージを再作成しない限りアプライアンスが稼働しなくなるため、ワイプアプライアンス機能は使用しないでください。

- ノードを追加または削除すると、クラスタのサイズとメンバーノードのロールによって、短時間停止することがあります。
- M3 サーバーのクラスタリングはサポートされていません。ご不明な点がありましたら、サポート ケースを開くまでお問い合わせください。
- 2.20 SMA アプライアンス リリース以降、2 ノード クラスタはサポートされていません。ノードが予期せずダウンした場合、2 つのノードではクォーラムを十分に維持できず、タイブレーカー ノードの以前のサポートがあっても、可用性の保証はありません。

要 件

重要 **エアギャップ展開でのクラスタリングは強く非推奨**：デバッグの複雑さが増大するため、エアギャップ展開や、顧客がデバッグへの L3 サポートアクセスを提供できない、または提供を望まないシナリオでは、アプライアンスのクラスタリングは**推奨されません**。

Cisco Secure Malware Analytics アプライアンスをクラスタリングする場合は、次の要件を満たす必要があります。

- **バージョン**：サポートされている設定でクラスタをセットアップするには、すべての Cisco Secure Malware Analytics アプライアンスが同じバージョンを実行している必要があります。常に使用可能な最新のバージョンにしておきます。
- **Clust インターフェイス**：各 Cisco Secure Malware Analytics アプライアンスには、クラスタ内の他の Cisco Secure Malware Analytics アプライアンスへのダイレクトインターコネクトが必要です。クラスタ内の各 Cisco Secure Malware Analytics アプライアンスの Clust インターフェイススロットに SFP+ を設置する必要があります（スタンドアロン構成の場合には該当しません）。

  ダイレクトインターコネクトとは、すべての Cisco Secure Malware Analytics アプライアンスが同じレイヤ 2 ネットワークセグメント上にあり、他のノードに到達するためのルー

ティングが不要で、大幅な遅延やジッターがないことを意味します。ノードが単一の物理ネットワーク セグメント上にないネットワーク トポロジはサポートされていません。

- **データ**： Cisco Secure Malware Analytics アプライアンスは、データが含まれていない場合にのみクラスタに結合できます（初期ノードのみがデータを保持できます）。既存の Cisco Secure Malware Analytics アプライアンスをデータのない状態に移行するには、データベース リセット プロセスを使用する必要があります（v2.2.4 以降で使用可能）。

重要 破壊的なワイプアプライアンスプロセスを使用しないでください。このプロセスにより、すべてのデータが削除され、シスコに返却してイメージを再作成しない限りアプライアンスが稼働しなくなります。

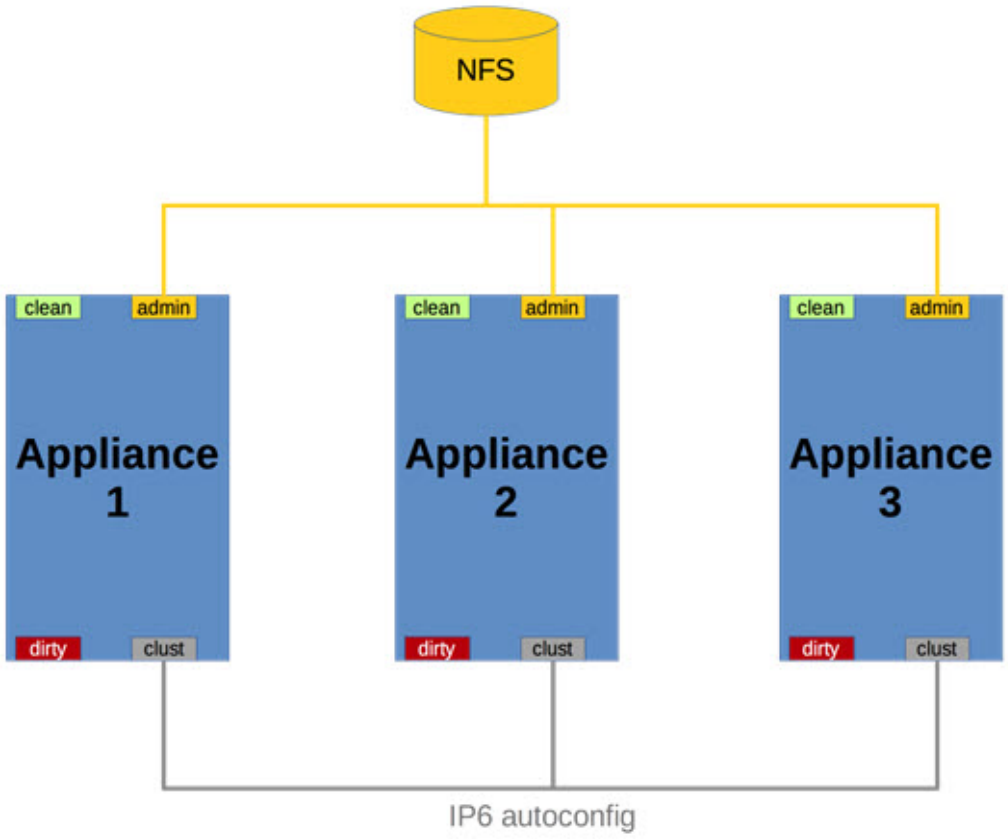
- **SSL 証明書**：1 つのクラスタノードにカスタム CA によって署名された SSL 証明書をインストールする場合、他のノードすべての証明書も同じ CA によって署名されている必要があります。

ネットワーキングと NFS ストレージ

Cisco Secure Malware Analytics アプライアンスをクラスタリングするには、ネットワーキングおよび NFS ストレージに関して次の点を考慮する必要があります。

- Cisco Secure Malware Analytics アプライアンスクラスタでは、NFS ストアを有効にして設定する必要があります。NFS ストアが管理インターフェイス経由で使用可能で、すべてのクラスタノードからアクセス可能になっている必要があります。
- 各クラスタは、キーが 1 つある 1 つの NFS ストアによってバックアップする必要があります。既存の Cisco Secure Malware Analytics アプライアンスのデータを使用して NFS ストアを初期化することはできますが、クラスタの動作中は、クラスタのメンバーではないシステムからアクセスすることはできません。
- NFS ストアはシングルポイント障害であり、そのロールに見合った、冗長性があり信頼性の高い機器を使用することが不可欠です。
- クラスタリングに使用される NFS ストアは、遅延を常に低い状態に保つ必要があります。

図 *52 :* クラスタリングネットワーク構成図



Cisco Secure Malware Analytics アプライアンス クラスタの構築

サポートされている方法で Cisco Secure Malware Analytics クラスタを構築するには、すべてのメンバーが同じバージョンである必要があります。バージョンは利用可能な範囲で常に最新のものにする必要があります。これは、すべてのメンバーが完全に更新されるように最初にスタンドアロンを構築する必要があることを意味します。

クラスタリングの前に Cisco Secure Malware Analytics アプライアンスがスタンドアロン アプライアンスとして使用されている場合、最初のメンバーのデータのみを保持できます。その他は構築の一部としてリセットする必要があります。

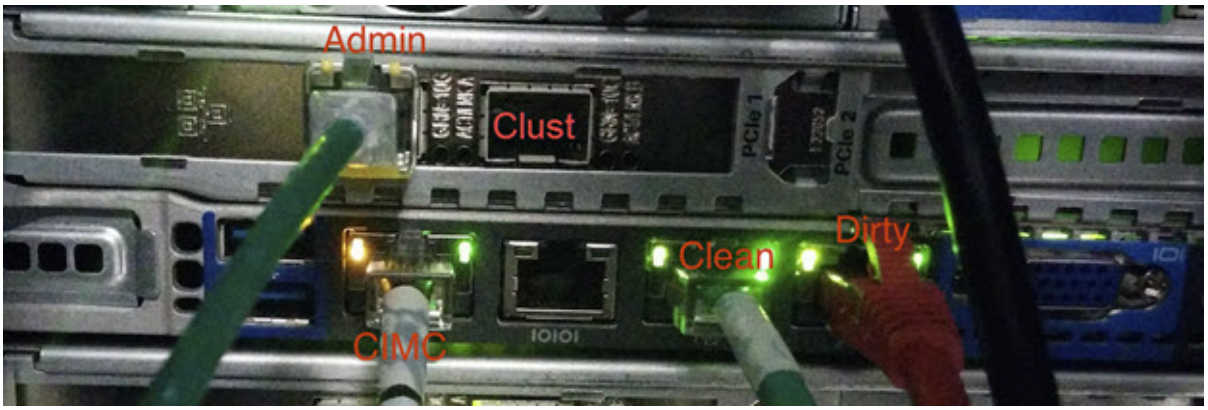
最初のノードで新しいクラスタを開始し、他の Cisco Secure Malware Analytics アプライアンスを結合します。新しいクラスタを構築するために使用できる 2 つの異なるパスがあります。

- 既存のスタンドアロン アプライアンスからのクラスタ構築の開始
- 新しいアプライアンスを使用したクラスタ構築の開始

Clust インターフェイスの設定

クラスタ内の各アプライアンスには、Clustインターフェイス用のSFP+を追加する必要があります。4番目の（非管理）SFPポートにSFP+モジュールを取り付けます。M5では、これは左から2番目のSPFインターフェイスです（詳細については、『Cisco Threat Grid M5 Hardware Installation Guide』を参照してください）。

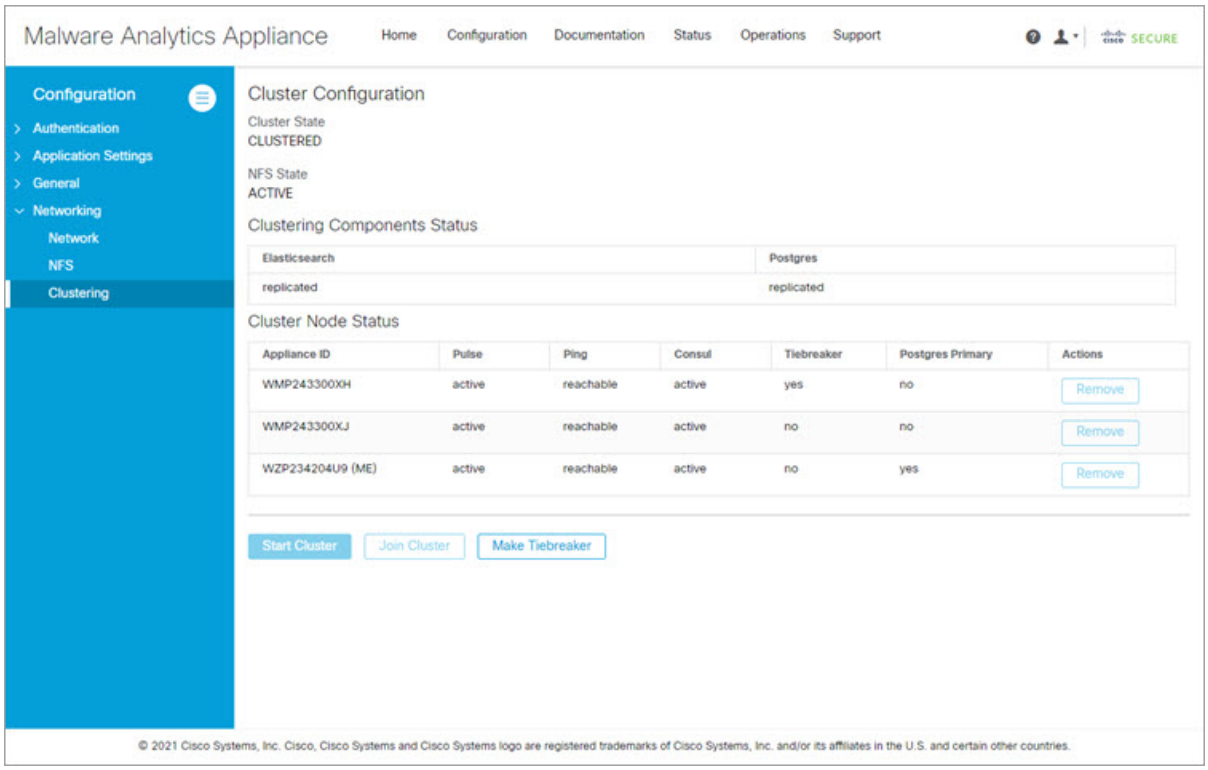
図 *53 : Cisco UCS M4 C220* の *Clust* インターフェイスの設定



クラスタの設定

クラスタは、**[クラスタ構成（Cluster Configuration）]**ページ（[構成（Configulation）]>**[ネットワーキング（Networking）]>[クラスタリング（Clustering）]**）でAdmin UIで構成され、管理されます。このセクションでは、アクティブで正常なクラスタを理解するためのこのページのフィールドについて説明します（スクリーンショットには3つのノードを含むクラスタが示されます）。

図 *54* : アクティブ クラスタのクラスタ構成



クラスタの前提条件

- アプライアンスは完全に設定され、構成される必要があります。
- [NFS 状態（NFS State）] が **[現用系（Active）]** でなければなりません。

クラスタの状態

- **[非構成（Unconfigured）]**：クラスタの一部として、またはスタンドアロンの Cisco Unconfigured アプライアンスとして明確に設定されていません。クラスタリングの前提条件が満たされている場合は、初期セットアップウィザードでこの選択を行います。
- **[Pending_NFS_Enable**：クラスタは NFS の有効化を保留中です。
- **Pending_NFS_Key**：クラスタは NFS キーを保留中です。
- **スタンドアロン（Standalone）** - アプライアンスはスタンドアロンノードとして構成されています。リセットしないとクラスタの一部として設定できません。
- **[クラスタ化（Clustered）]**：他の 1 つ以上の Cisco Secure Malware Analytics アプライアンスでクラスタ化されています。
- **[不明（Unknown）]**：ステータスを特定できません。

コンポーネント ステータスのクラスタリング

- **[Elasticsearch]**：検索機能を必要とするクエリに使用されるサービス。
- **[PostgreSQL]**：最新の確定的なデータ（アカウントルックアップなど）が必要なクエリに使用されるサービス。

両方のサービスは、次のステータス値のいずれかで説明されます。

- [**Replicated**]：すべてが正常に動作しています。また、障害時に引き継ぎに必要なすべてのものも所定の位置にあります。アプライアンスは障害を許容して操作を続行できます。複製済みの状態は、障害発生時のダウンタイムがゼロになるという意味ではありません。むしろ、障害には、ゼロのデータ損失と制約ダウンタイムが伴います（通常の状況で1分未満、失敗した特定のクラスタ ノードでのアクティブな分析を除く）。

  ノードがダウンするメンテナンス操作は、クラスタが複製された状態のときにのみ実行する必要があります。

  完全に複製されたクラスタの場合、リカバリは自動的に行われ、通常のシナリオで完了するのに必要な時間は 1 分未満です。
- [**Available**]：すべてが正常に動作しており、参照サービスを使用できます（APIおよびユーザー要求を処理できます）が、複製されません。
- [**Unavailable**]：非機能サービスとして知られています。

詳細については、Cisco.com の「*Cisco Secure Malware Analytics アプライアンス Clustering FAQ*」を参照してください。

クラスタ ノード ステータス

- [**Pulse**]：（初期設定中ではなく、サービスを実行している間に）ノードがアクティブに接続されていて、NFS ストアを使用しているかどうかを示します。
- [**Ping**]：Clust インターフェイス上でクラスタノードを認識できるかどうかを示します。
- [**Consul**]：ノードがコンセンサスストアに参加しているかどうかを示します。参加には、Clust でのネットワーク接続と互換性のある暗号キーの両方が必要です。
- **[Postgres プライマリ（Postgres Primary）]** - ノードが PostgreSQL プライマリ ノードであるかどうかを示します。

既存のスタンドアロン アプライアンスからのクラスタ構築の開始

Cisco Secure Malware Analytics Appliance のクラスタの構築を開始するときは、最初のノードを既存のスタンドアロン Cisco Secure Malware Analytics Appliance または新しいアプライアンスにしてクラスタを開始する必要があります。ここでは、既存のスタンドアロン Cisco Secure Malware Analytics アプライアンスからクラスタを構築する方法について説明します。これにより、あるアプライアンスから既存のデータを保持し、そのアプライアンスを使用して新しいクラスタを開始できます。

（注）
- クラスタが開始される NFS で、既存のバックアップが使用可能になっている必要があります。
- クラスタに結合される他のすべてのノードから、結合前にデータを削除する必要があります。追加されるノードのデータをクラスタにマージすることはできません。
- v2.4.3 よりも前のリリースで、NFS にバックアップされたデータを含むスタンドアロン Cisco Secure Malware Analytics アプライアンスの場合、新しいクラスタの初期ノードにするために、データベースのリセットとバックアップからの復元を行う必要がなくなりました。以前のバージョンの Cisco Secure Malware Analytics アプライアンスをお持ちの場合、新しいクラスタを開始する前に、v2.4.3 以降にアップグレードしてからリセット操作を実行することをお勧めします。

既存のスタンドアロンアプライアンスからクラスタ内の最初のノードの構築を開始するには、次の手順を実行します。

手順

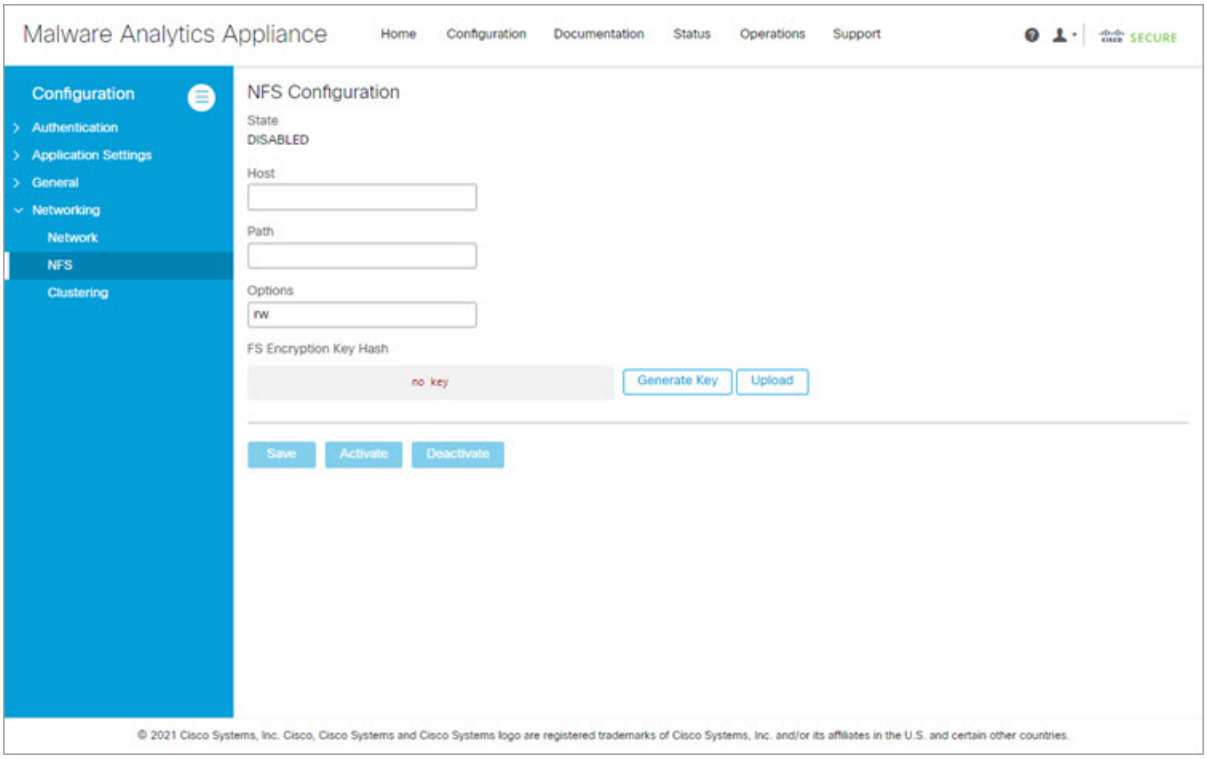
ステップ 1 Cisco Secure Malware Analytics アプライアンスを最新バージョンに完全に更新します。現在実行されているバージョンによっては、最新バージョンになるまでに複数の更新サイクルが必要になる場合があります。

ステップ 2 まだ完了していない場合は、アプライアンスのバックアップのための NFS を設定します。

（注）
この手順では、デフォルトの Linux NFS サーバーの実装について説明します。お使いのサーバーのセットアップによって異なる場合があります。

a) [構成（Configuration）] タブをクリックします。
b) サイドナビゲーションで **[ネットワーキング（Networking）]** を展開し、 **[NFS]** を選択して **[NFSの構成（NFS Configuration）]** ページを開きます。

図 *55 : NFS* の設定



c) 次のフィールドに入力します。

- [**Host**]：NFSv4 ホストサーバー。IP アドレスを使用することをお勧めします。
- [**Path**]：ファイルが保存される NFS ホストサーバー上の場所への絶対パス。これにはキー ID サフィックスは含まれません。自動的に追加されます。
- **オプション**：このサーバーで NFSv4 に対する標準 Linux のデフォルト値を変更する必要がある場合に使用される NFS マウントオプション。

d) [保存（Save）] をクリックします。

ページが更新され、**[キーの生成（Generate Key）]** ボタンが使用可能になります。

このページを初めて構成するときに、暗号キーの削除とダウンロードのための暗号キーの **[削除（Remove）]** ボタンと **[ダウンロード（Download）]** ボタンが表示されます。

[アップロード（Upload）] ボタンは、NFS が有効になっているものの、キーが作成されていない場合に使用できます。キーを作成すると、[**Upload**] ボタンが [**Download**] ボタンに変わります。キーを削除すると、**[ダウンロード（Download）]** ボタンが **[アップロード（Upload）]** ボタンに戻ります。

（注）
このキーがバックアップの作成に使用されたキーと正確に一致する場合、アップロード後に Admin UI に表示される**キー ID** は、設定されたパス内のディレクトリ名と一致している必要があります。暗号キーを使用せずにバックアップを復元することはできません。設定プロセスには、NFS ストアお

よび暗号化データをマウントするプロセスと、NFS ストアのコンテンツからアプライアンスのローカル データストアを初期化するプロセスが含まれます。

e) [キーの生成（Generate Key）] をクリックして、新しい NFS 暗号キーを作成します。

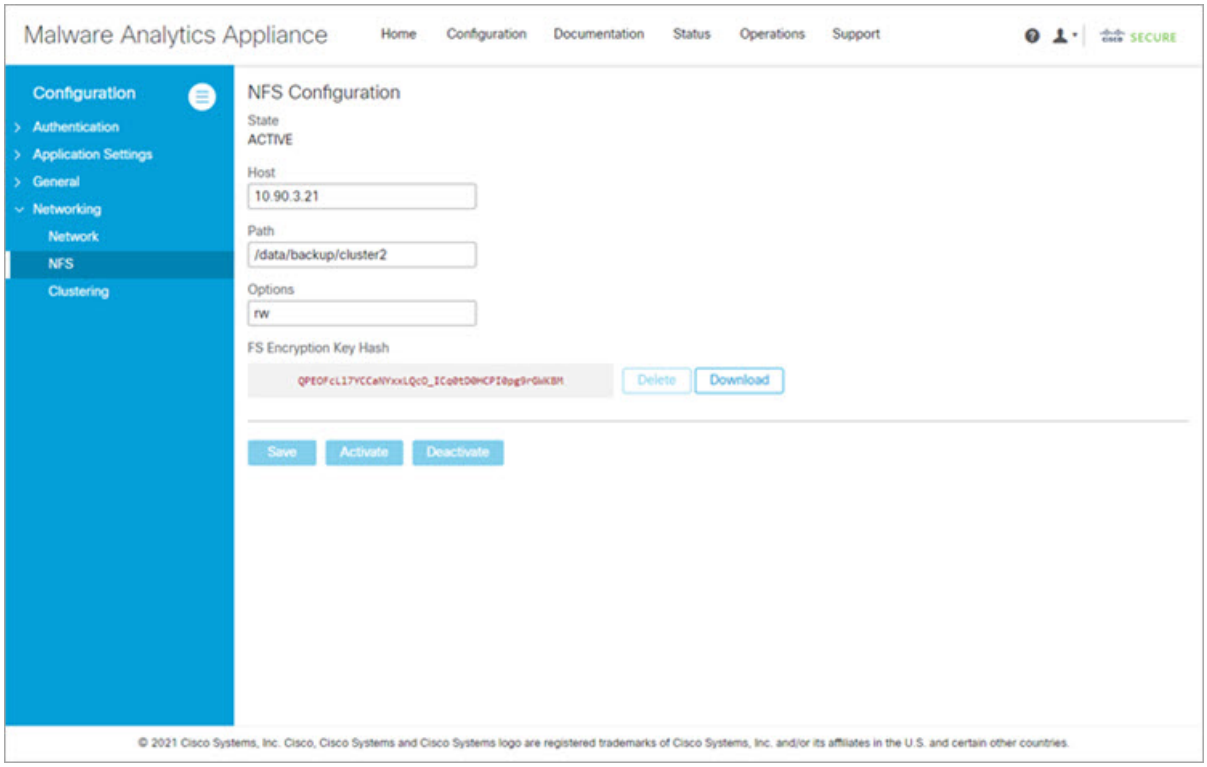
f) [保存（Save）] をクリックします。

ページが更新されて **[キー ID]** が表示され、**[Activate]** ボタンと **[ダウンロード（Download）]** ボタンが使用可能になります。

g) [Activate] をクリックします。

数秒後、**[状態（State）]** が**[現用系（Active）]** になります。

図 *56 : [Active]* になった *NFS*



h) [**Download**] をクリックして、バックアップの暗号キーをダウンロードします。安全な場所に生成したファイルを保存します。クラスタに追加のノードを結合するためのキーが必要です。

重要
この手順を実行しないと、次の手順ですべてのデータが失われます。

ステップ 3 必要に応じて設定を完了し、Cisco Secure Malware Analytics アプライアンスを再起動して、NFS バックアップ設定を適用します。

ステップ 4 バックアップを実行します。

（注）

推奨どおりに、前もって少なくとも48時間バックアップを実行し、バックアップに問題が発生したことを示すサービス通知がなかった場合、次の手動による手順は不要です。

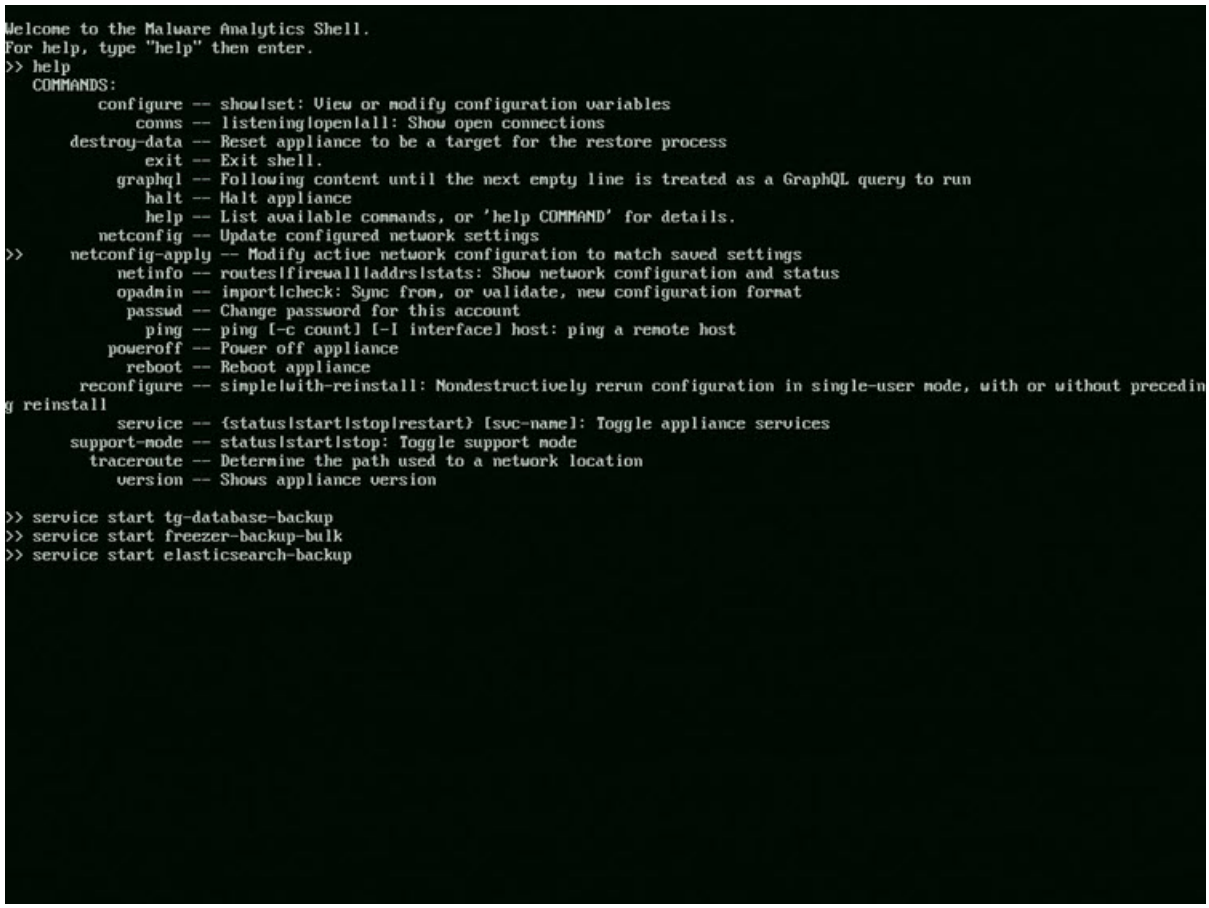
バックアップなどのサービス通知は、Cisco Secure Malware Analytics Portal UI の右上隅にあるアイコンで表示できます。「**There is no PostgreSQL backup yet（PostgreSQL バックアップがまだありません）**」というサービス通知が表示された場合は、手順を先に進めないでください。

48 時間待たずにバックアップを使用できるようにする場合は、NFS へのすべてのデータのバックアップを手動で開始して、完了を確認します。手動バックアップの実行は、スタンドアロン アプライアンスをクラスタに再構築する直前にバックアップを設定する場合にのみ必要です。

a) **TGSH** を開き、次のコマンドを入力します。

```
service start tg-database-backup.service
service start freezer-backup-bulk.service
service start elasticsearch-backup.service
```

図 *57 : NFS* に対する全データのバックアップの開始



b) 最後のコマンドが返された後、約 5 分間待機します。

ステップ 5 Cisco Secure Malware Analytics ポータル UI で、サービス通知を確認します。任意の通知に、PostgreSQL バックアップがまだありませんという警告などのバックアップ プロセスの障害が示されている場合は、続行しないでください。

重要
上述のプロセスが正常に完了しない限り、手順を先に進めないでください。

ステップ 6 [構成（Configuration）] タブをクリックします。

ステップ 7 サイドナビゲーションで**[ネットワーキング（Networking）]**を展開し、**[クラスタリング（Clustering）]**を選択して**[クラスタリングの構成（Clustering Configuration）]**ページを開きます。

ステップ 8 [**Start Cluster**] をクリックします。

ステップ 9 確認ダイアログで、[OK] をクリックします。

[**Clustering Status**] が [**Clustered**] に変わります。

ステップ 10 インストールを終了します。この操作により、クラスタモードでデータの復元が開始されます。

次のタスク

「クラスタへの Cisco Secure Malware Analytics アプライアンスの結合」で説明されているように、他の Cisco Secure Malware Analytics アプライアンスの新しいクラスタへの結合を開始できます。

新しいアプライアンスを使用したクラスタ構築の開始

Cisco Secure Malware Analytics アプライアンスのクラスタの構築を開始する場合、最初のノードが新しい Cisco Secure Malware Analytics アプライアンスであるクラスタを開始できます。このクラスタ構築の方法は、ソフトウェアのクラスタ対応バージョンに同梱されている新しいアプライアンス、またはデータをリセットした既存のアプライアンスに使用できます。

（注） 「バックアップ復元ターゲットとしての Cisco Secure Malware Analytics アプライアンスのリセット」に記載されているとおり、`destroy-data` コマンドを使用して既存のデータを削除します。アプライアンスのワイプ機能は使用しないでください。

手順

ステップ 1 通常どおり Admin UI 構築を設定および開始します。

ステップ 2 [ネットワーク] と [ライセンス] を設定します。

ステップ 3 [構成（Configuration）] タブをクリックします。

ステップ 4 サイドナビゲーションで **[Networking]** を展開し、 **[NFS]** を選択して **[NFSの構成（NFS Configuration）]** ページを開きます。

（注）
「既存のスタンドアロン アプライアンスからのクラスタ構築の開始」の図を参照してください。

ステップ 5 次のフィールドに入力します。

- [**Host**]：NFSv4 ホストサーバー。IP アドレスを使用することをお勧めします。
- [**Path**]：ファイルが保存される NFS ホストサーバー上の場所への絶対パス。これにはキー ID サフィックスは含まれません。自動的に追加されます。
- **オプション**：このサーバーで NFSv4 に対する標準 Linux のデフォルト値を変更する必要がある場合に使用される NFS マウントオプション。

ステップ 6 [保存（Save）] をクリックします。

ページが更新されます。**[キーの生成（Generate Key）]** ボタンと **[アクティブ化（Activate）]** ボタンが使用できるようになります。

ステップ 7 [キーの生成（Generate Key）] をクリックして、新しい NFS 暗号キーを作成します。

ステップ 8 [Activate] をクリックします。

[状態（State）] が **[アクティブ（Active）]** に変わります。

ステップ 9 [Download] をクリックして、保管のために暗号キーのコピーをダウンロードします。クラスタに追加のノードを結合するためのキーが必要です。

ステップ 10 **[クラスタの構成（Cluster Configuration）]** ページで **[クラスタの開始（Start Cluster）]** をクリックしてから、確認ダイアログで **[OK]** をクリックします。

[クラスタの状態（Clustering State）] が [クラスタ化（Clustered）] に変わります。

ステップ 11 ウィザードの残りの手順を完了し、**[Start Installation]** をクリックします。この操作により、クラスタモードでデータの復元が開始されます。

ステップ 12 **[クラスタの構成（Cluster Configuration）]** ページを開き、新しいクラスタの正常性を確認します。

次のタスク

クラスタへの Cisco Secure Malware Analytics アプライアンスの結合に進みます。

クラスタへの Cisco Secure Malware Analytics アプライアンスの結合

このセクションでは、新規または既存の Cisco Secure Malware Analytics アプライアンスをクラスタに結合する方法について説明します。

（注） Cisco Secure Malware Analytics アプライアンスは、データが含まれていない場合にのみ、既存のクラスタに結合できます。データが含まれている可能性のある最初のアプライアンスの場合とは異なります。

また、クラスタに結合している Cisco Secure Malware Analytics アプライアンスに最新のソフトウェアバージョンがインストールされていることは非常に重要です（クラスタ内のすべてのノードが同じバージョンを実行している必要があります）。これは、最初に Cisco Secure Malware Analytics アプライアンスを設定することが必要です。その後そのデータをリセットして、クラスタに結合します。

一度に 1 つのノードを追加するようにし、次のノードを追加する前に、Elasticsearch と PostGres が [**レプリケーション済み（Replicated）**] の状態になるまで待機します。[**Replicated**] のステータスは、2 つ以上のノードを含むクラスタで想定されています。

（注） Elasticsearch および PostgreSQL の状態が **[レプリケーション済み（Replicated）]** に変更されるまでの待機時間は、単一ノードの場合には当てはまりません。バックアップから単一ノードクラスタを初期化する場合は、復元が完了し、アプリケーションが UI に表示されるのを待ってから、2 番目のノードを追加する必要があります。

クラスタに Secure Malware Analytics アプライアンスを結合するとき、初期設定時に NFS とクラスタリングが構成される必要があります。

既存のアプライアンスのクラスタへの結合

Perform the following steps to join an 既存の Secure Malware Analytics アプライアンスをクラスタに結合するには、次の手順を実行します。

手順

ステップ 1 Secure Malware Analytics アプライアンスを最新バージョンに更新します。この手順では、インストールされている現在のバージョンに応じて、複数の更新サイクルが必要になる場合があります。クラスタ内のすべてのノードを同じバージョンにする必要があります。

ステップ 2 すべてのデータを削除するには、`tgsh` で **destroy-data** コマンドを実行します。既存の Secure Malware Analytics アプライアンスをクラスタに結合する際、クラスタにマージする前に、すべてのデータを削除する必要があります。バックアップ復元ターゲットとしての Cisco Secure Malware Analytics アプライアンスのリセット参照してください。

既存の Secure Malware Analytics アプライアンスで `destroy-data` コマンドを実行した後、このアプライアンスは基本的に新しいノードになるため、クラスタに結合するには、新しいアプライアンスのクラスタへの結合場合と同じ手順に従います。

新しいアプライアンスのクラスタへの結合

既存の Cisco Secure Malware Analytics アプライアンスをクラスタに結合するには、次の手順を実行します。

手順

ステップ 1 『Cisco Secure Malware Analytics アプライアンス スタート ガイド』の説明に従って、新しい Admin UI の構成を開始します。

ステップ 2 **[NFSの設定（NFS Configuration）]** ページで、クラスタ内の最初のノードに入力した設定と一致するように **[ホスト（Host）]** と **[パス（Path）]** を指定します。

ステップ 3 **FS Encryption Key Hash** の**[アップロード]** をクリックし、新しいクラスタを開始した際の最初のノードからダウンロードした NFS 暗号キーを選択します。

ステップ 4 **[保存（Save）]** をクリックします。

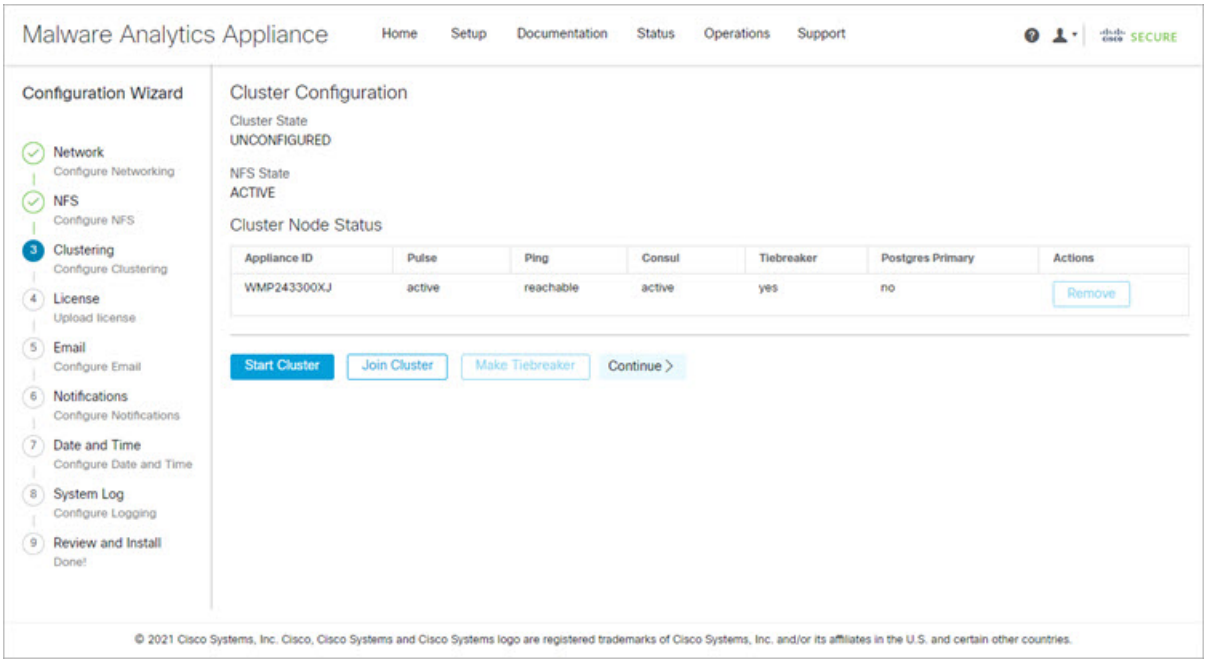
ページが更新されます。[**Key ID**] が表示され、[**Activate**] ボタンが有効になります。

ステップ 5 [続行（Continue）] をクリックします。

[クラスタ構成（Cluster Configuration）] 画面が最初のノードで表示されます。

ステップ 6 [**Join Cluster**] をクリックしてから、確認ダイアログで [**OK**] をクリックします。

図 *58 :* クラスタの設定



[クラスタの状態（Cluster State）] が [クラスタ化（Clustered）] に変わります。

ステップ 7 クラスタに結合するノードごとに、手順 1 ～ 手順 10 を繰り返します。

クラスタ ノードの削除

クラスタからノードを削除するには、**[クラスタ設定（Cluster Configuration）]** ページ（**[設定（Configuration）]>[クラスタリング（Clustering）]**）に移動し、削除するノードの **[アクション（Action）]** 列で **[削除 （Remove）]** をクリックします。

- クラスタからノードを削除するとは、ノードが一時的にダウンするということではなく、クラスタの一部と見なされなくなることを意味します。Cisco Secure Malware Analytics アプライアンスは、使用を停止している間に削除する必要があります。削除されたアプライアンスは、別のハードウェアに置き換えられるか、データがリセットされた後にのみクラスタに再度結合されます。
- ノードの削除は、ノードを再度追加しないユーザーの意向をシステムに伝えることに相当します。再度追加しようとすると、ノードがリセットされます。
- ノードは、パルスがある（NFS にアクティブに書き込まれている）場合、または consul（合意ストアの一部）でアクティブになっている場合、クラスタから完全に削除されたものとしてマークされません。

（7 ノード未満のクラスタ内の）ライブになっているノードを置き換えるには、新しいノードを追加し、クラスタが緑色になるのを待ってから、**[Remove]** ボタンを使用して古いノードをオフラインにします。この操作は、ノードを戻さない意向をシステムに伝えることに相当します。

ノードをオフラインにすると、クラスタのステータスは黄色に変わります。**[Remove]** をクリックすると、ステータスが緑色に戻ります（削除されたばかりのノードの存在が想定されなくなり、クラスタのサイズが変更されるため）。

ヒント 欠落している（障害があるか、電源が切れている）ノードは、最終的にタイムアウトになり、削除できるようになります。

クラスタのサイズ変更

[削除（Remove）] ボタンを使用してクラスタからノードが削除されると、クラスタのサイズが変更されます。その結果、許容される障害の数に影響が及ぶ場合があります。許容される障害の数（障害許容範囲で定義）が変わるほど大きくクラスタのサイズが変更されると、Elasticsearch が強制的に再起動され、サービスが一時的に中断されます。

例外：上記には、再起動中か、一時的な障害が発生している PostgreSQL マスター以外のシステムは含まれません。中断は、そのノードをアクティブに使用したクライアントを除くケースで、またはサンプルを実行している場合は、最小限にする必要があります。

すでにクラスタの一部ではない Secure Malware Analytics アプライアンスを追加する場合、または **[削除（Remove）]** をクリックする場合、許容される障害の数が変更されるなどクラスタのサイズが変更され、クラスタの残りが再設定するときに一時的に中断されます。

障害許容範囲

障害が発生した場合、クラスタ化された Cisco Secure Malware Analytics アプライアンスは、失敗したノードによってアクティブに実行されている分析の例外でデータを失うことはありません。最小限（1 分未満）のサービス中断期間でユーザーの関与なくサービスを回復します。

使用可能なノードの数が [**Failure Tolerances**] テーブルの [**Nodes Required**] 列に表示されている数以上である場合、ほとんどの障害は1分未満で回復します。または、使用可能なノードの数が増えて前述の数を満たすようになると回復します。この条件は、障害発生前にクラスタが正常な状態だった場合に当てはまります（[**Clustering**] ページで [**Replicated**] と表示されるサービスによって示される）。

特定のサイズのクラスタが許容すると想定される障害の数を次の表に示します。

表 *3 :* **障害許容範囲**

クラスタ サイズ	許容される障害	必要なノード
1	0	1
3	1	2
4	1	3
5	2	3
6	2	4
7	3	4

次の図は、最良のシナリオを表します。すべてのノードがアップするときにクラスタがボード上で緑色に表示されない場合、示された完全な障害の数を許容できない場合があります。

たとえば、2 つの障害が許容される 5 ノードのクラスタサイズを使用しており、3 つのノードが必要で、5 台のアプライアンスすべてがアクティブにデータを処理しているときに、2 つまでの障害が発生した場合、クラスタは自動的に再設定され、手動による管理アクションなしで動作を続行できます。

別の考慮事項として、5、6、または 7 ノードのクラスタの場合、許容される障害の数が 1 つ増えるごとに、障害が発生し得るノードの比率が高くなることを意味します。この事実は、ノードの数が障害発生率の乗数となるため、特に重要です。（2 つのノードを使用していて、各々にハードウェア障害が 10 年ごとに発生している場合は、ハードウェアの障害発生率を 5 年間に 1 回に変更します）。

障害の回復

多くの場合、障害が発生しても自動的に回復します。回復しない場合は、サポート ケースを開くに連絡するか、バックアップからデータを復元する必要があります。詳細については、「バックアップコンテンツの復元」を参照してください。

API/使用の特性

クラスタ内の任意のノードに送信されたサンプルのステータスは、クラスタ内の他のノードからクエリされることがあります。送信が行われる個々のノードを追跡する必要はありません。

1 つのノードに行われたサンプル送信の処理は、クラスタ内のすべてのノード間で分割されます。クライアント側からアクティブに負荷分散する必要はありません。

運用/管理の特性

フェールオーバーが発生している間にサービスが一時的に中断される可能性があります。フェールオーバー中にアクティブに実行されているサンプルは自動的に再実行されません。

クラスタリングのコンテキストでは、キャパシティとは、ストレージではなくスループットを意味します。3 つのノードを持つクラスタは、単一の Cisco Secure Malware Analytics アプライアンスと同じ最大ストレージレベルまでデータをプルーニングします。その結果、5000 サンプルアプライアンス 3 台を含むクラスタ（合計 15,000 サンプル/日のレート制限）は（フルキャパシティで使用されている場合）、Cisco.com の『*Threat Grid Appliance Data Retention Notes*』に記載されている 10,000 サンプル/日の想定よりも、最短保持期間が 33 % 短くなります。

サンプルの削除

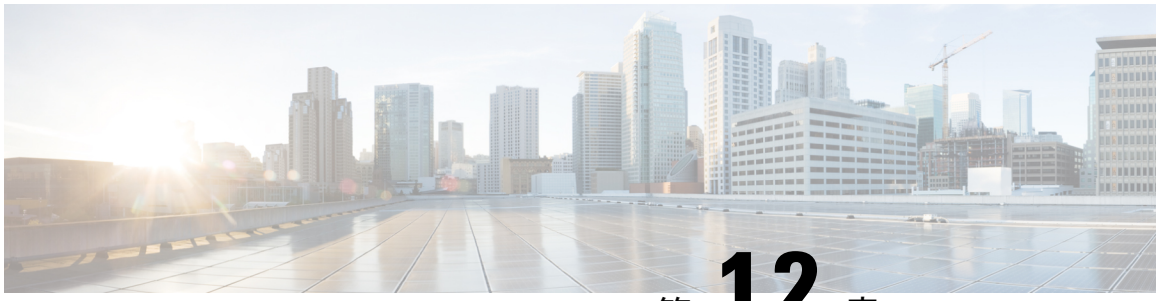
Cisco Secure Malware Analytics アプライアンス（v2.5.0 以降）では、サンプルの削除がサポートされます。

- [**Delete**] オプションは、サンプルリストの [**Actions**] メニューにあります。
- [**Delete**] ボタンは、サンプル分析レポートの右上隅にあります。

（注） 削除されたサンプルのバックアップコピーがすべてのノードから削除されるまでに、最大 24 時間かかる場合があります。

削除されたサンプルは、ただちに共有 NFS ストアから削除されます。削除要求を処理しているノードからはすぐに削除されますが、他のノードでは、夜間の cron ジョブが実行されるまで保留になります。クラスタモードでは、NFS ストアはサンプルのプライマリ ソースと見なされます。そのため、サンプルが他のノードから物理的に削除されていない場合でも、いずれのノードからも取得できなくなります。

Secure Malware Analytics アプライアンス バージョン2.7 以降では、クラウド製品の動作に合わせて、サンプルの削除にアーティファクトが含まれるように拡張されています。



第 12 章

ステータス

Admin UI の **[ステータス（Status）]** メニューは、インストールされているシステムパッケージとそのバージョン、詳細ログ、使用可能なストレージなどのシステム情報を表示するために管理者によって使用されます。

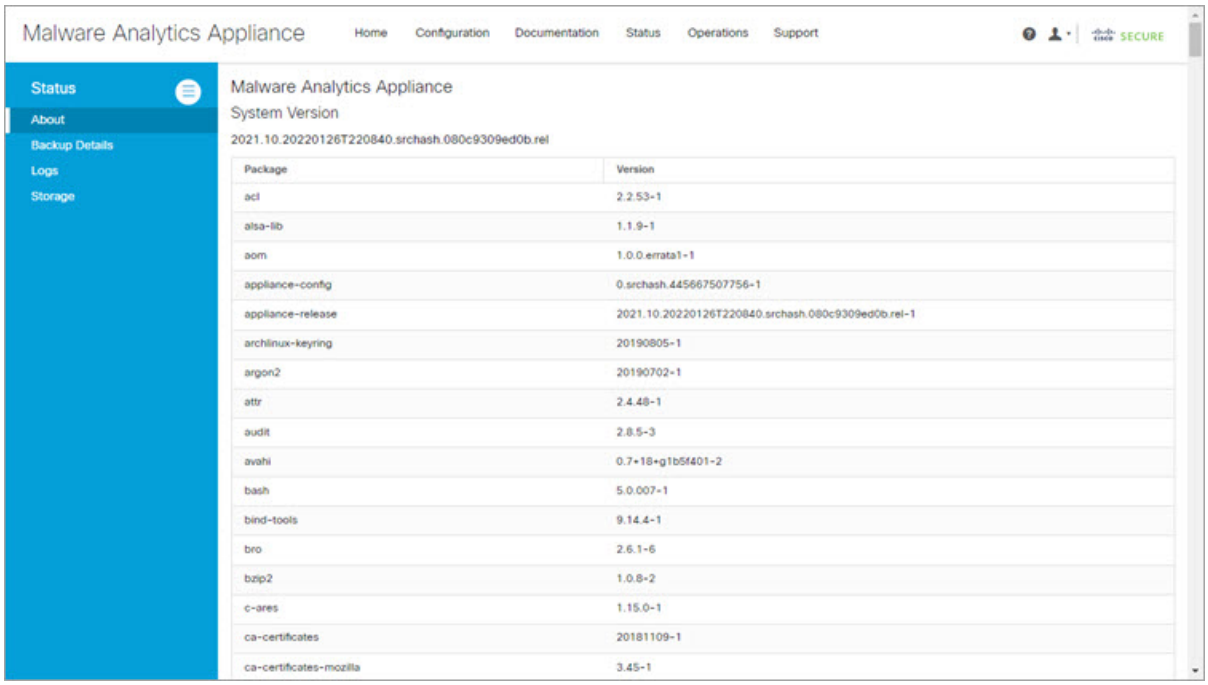
バージョン情報

インストールされているパッケージとそれらのバージョンは、管理 UI の **[システムバージョン（System Version）]** ページで確認できます。

手順

ステップ 1 **[ステータス（Status）]** タブをクリックして [バージョン **情報（About）]** を選択し、[**システムバージョン（System Version）]** ページを開きます。

図 *59 : System Version*



ステップ 2 インストールされているパッケージとそのバージョンを表示します。リリースバージョンは、ページの上部に表示されます。

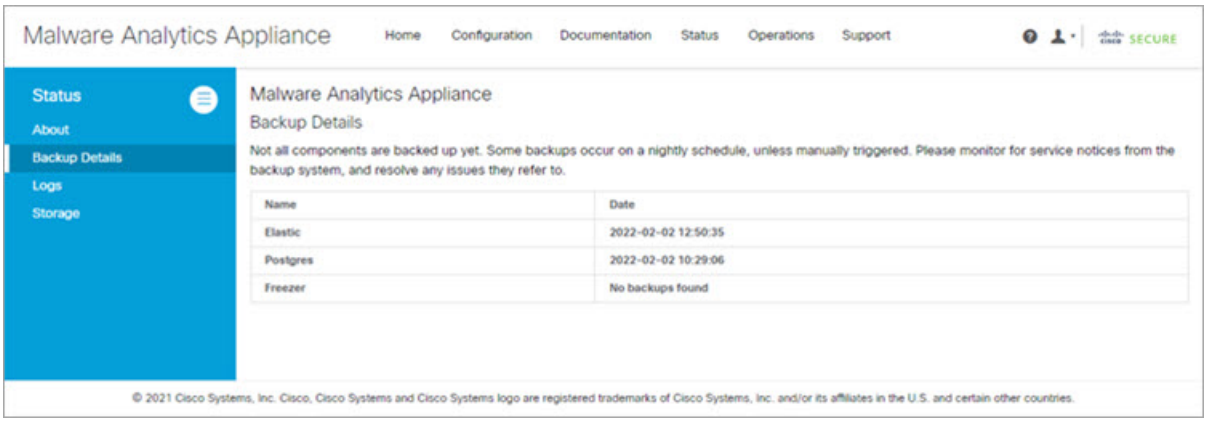
ビルド番号と対応するリリースバージョンを確認するには、「*Cisco Secure Malware Analytics アプライアンス バージョン ルックアップ テーブル*」を参照してください。

バックアップの詳細

[バックアップの詳細（Backup Details）] ページで詳細なバックアップ情報を表示できます。これには、PostgreSQL、Elasticsearch、Sand Castle フリーザーデータの完全な非増分バックアップ (該当する場合) が正常に完了した最新の時刻が表示されます。

[ステータス（Status）] タブをクリックして **[バックアップの詳細（Backup Details）]** を選択し、 **[バックアップの詳細（Backup Details）]** ページを開きます。

図 *60* : バックアップの詳細



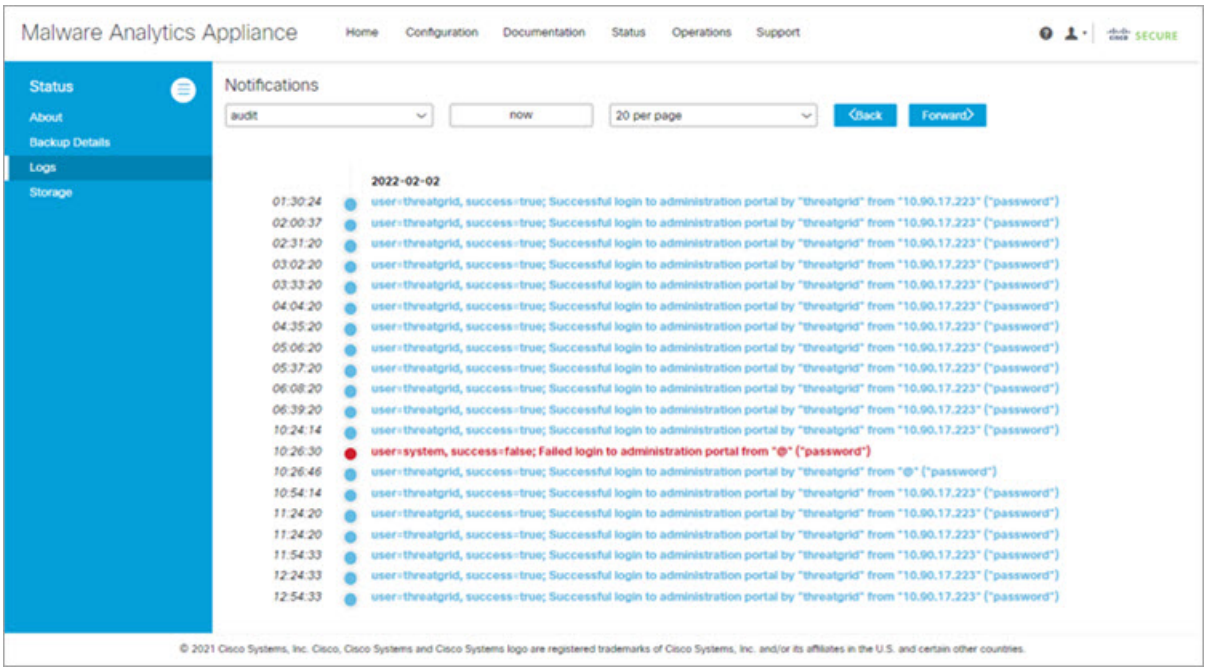
ログ

[通知（Notifications）] ページで、履歴システムログを含む詳細なログ情報を表示できます。

手順

ステップ 1 **[ステータス（Status）**] メニューをクリックし、 **[ログ（Logs）]** を選択して **[通知（Notifications）]** ページを開きます。

図 *61* : 通知



ステップ 2 ドロップダウン リストから通知のタイプを選択して表示されるログをフィルタリングし、ページに表示するレコード数を指定します。

ページ間の移動には、**[戻る（Back）]** ボタンと **[進む（Forward）]** ボタンを使用します。

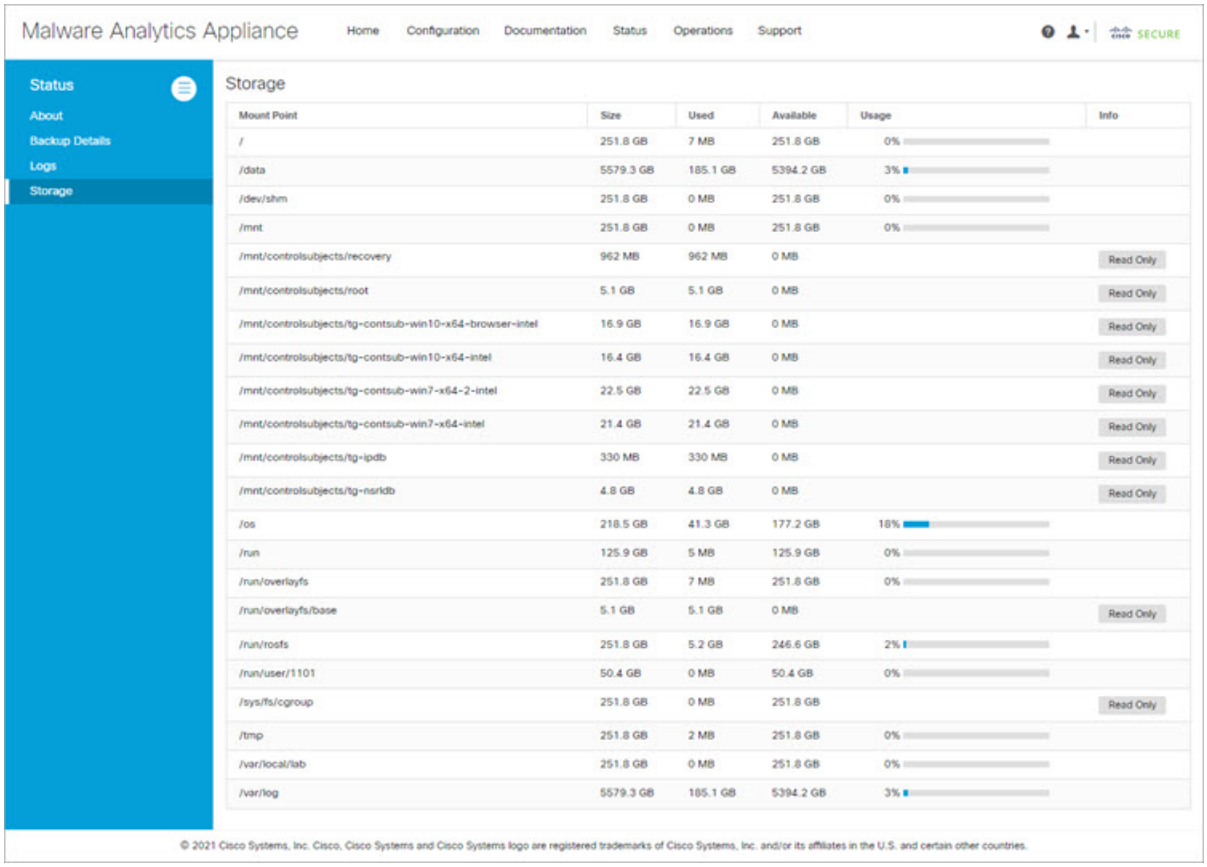
ストレージ

[ストレージ（Storage）] ページで、Cisco Secure Malware Analytics アプライアンスで使用可能なストレージを表示できます。

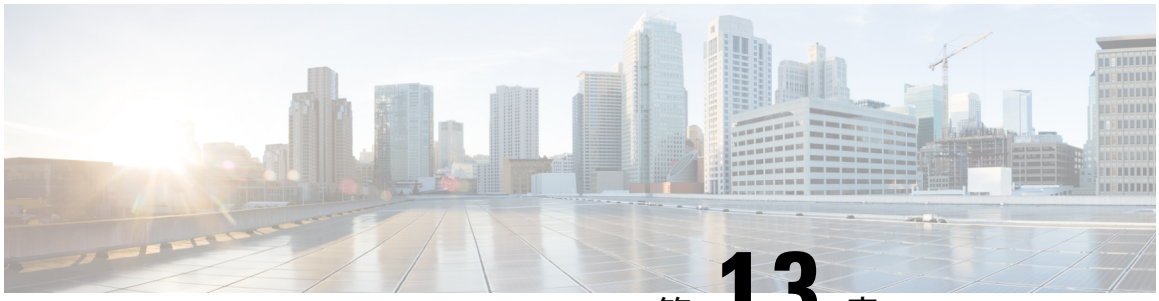
手順

ステップ 1 **[ステータス（Status）]** タブをクリックし、**[ストレージ（Storage）]**を選択します。

図 *62 :* ストレージ



ステップ 2 ディレクトリのサイズ、使用済みストレージの量、および使用可能なストレージ量を表示します。



第 13 章

操作

[操作（Operations）] メニューは、管理者が Cisco Secure Malware Analytics アプライアンスの操作タスクを実行するために使用します。この章では、設定変更のアクティブ化、Admin UI のリロード、ジョブと電源設定の管理、アプライアンスの更新を含むこれらのタスクについて説明します。

有効化

Admin UI の設定に対する変更は保存する必要があり、いくつかの変更を保存して再設定を行い、変更を確定する必要があります。設定の変更は、再設定が完了するまで有効になりません。

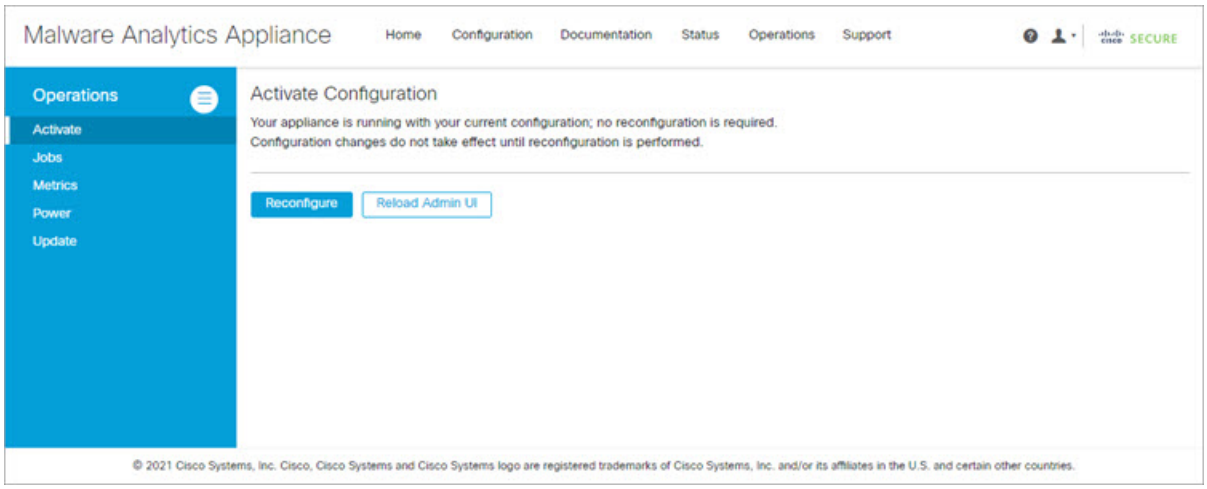
再構成が必要な場合、ページの上部にあるバナーに、薄いオレンジ色のアラートメッセージが表示されます。このバナーの **[再設定（Reconfigure）]** ボタンをクリックすると、**[操作（Operations）]** メニューの **[構成のアクティブ化（Activate Configuration）]** ページに移動します。このページから、構成の変更を適用し、Admin UI をリロードすることもできます。

手順

ステップ 1 アラートメッセージの **[再構成（Reconfigure）]** をクリックして、再構成プロセスを開始します。

ステップ 2 **[構成のアクティブ化（Activate Configuration）]** ページで、**[再構成（Reconfigure）]** をクリックして再構成ジョブを実行します。

図 *63 :* 構成をアクティブ化する



ステップ 3 確認ダイアログで、**[再構成（Reconfigure）]** をクリックして再構成ジョブを開始します。

構成がアクティブ化され、その進行状況に関するメッセージが [ジョブ（Jobs）] ウィンドウに表示されます。エラーメッセージやその他の情報を確認する必要がある場合は、詳細がジョブ（Jobs）ページに保持されます。

完了すると、再構成が成功したことを示す確認メッセージが表示されます。

ステップ 4 [続行（Continue）] をクリックします。

ステップ 5 Admin UI を更新する場合は、**[Admin UIのリロード（Reload Admin UI）]**をクリックします。

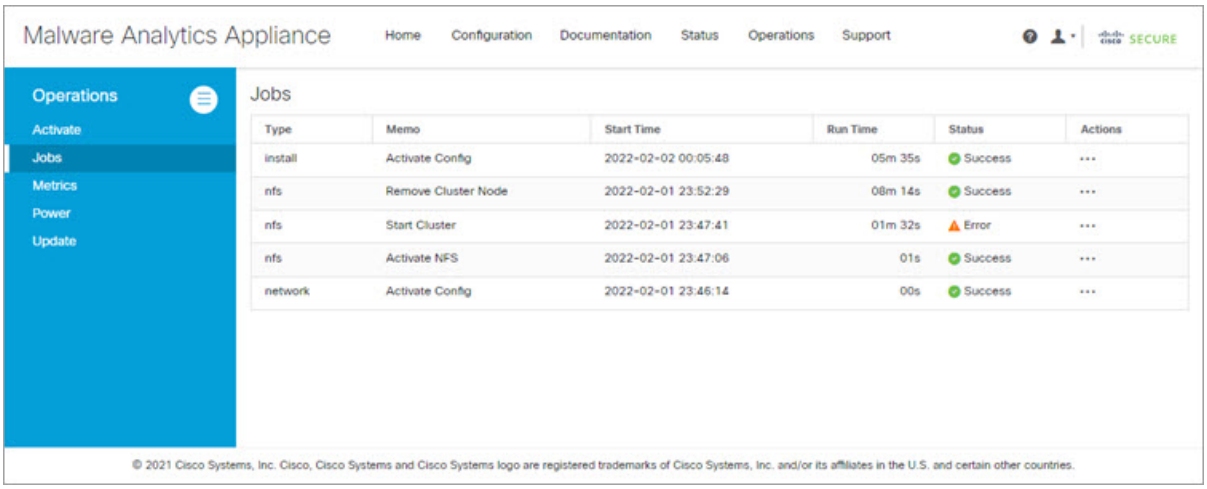
ジョブ（Jobs）

管理 UI の **[ジョブ（Jobs）]** ページを使用して、Cisco Secure Malware Analytics アプライアンスで実行されたジョブを表示できます。このページを使用して、特定のジョブに関するエラーメッセージやその他の情報を表示できます。

手順

ステップ 1 **[操作（Operations）]** タブをクリックし、**[ジョブ（Jobs）]**を選択します。

図 *64 :* ジョブ（*Jobs*）



各ジョブのジョブタイプ、開始時刻、実行時間、およびステータスが表示されます。

ステップ 2 ジョブの情報を表示するには、**[アクション（Actions）]** 列の小さい **[詳細（Details）]** ボタンをクリックします。

電源

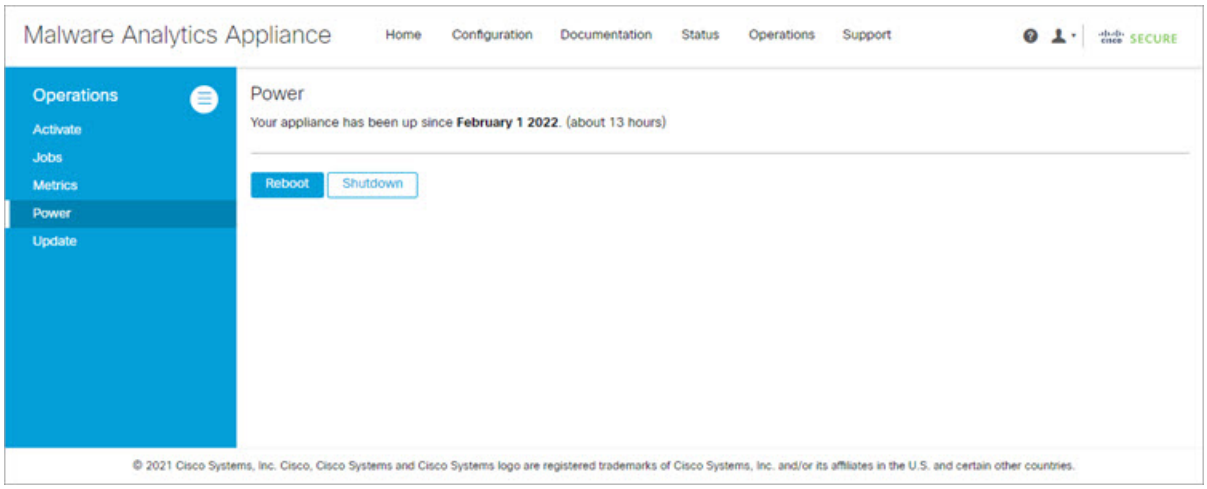
管理 UI の **[電源（Power）]** ページから Cisco Secure Malware Analytics アプライアンスを再起動またはシャットダウンできます。

（注） GNU GRUB ブートローダーが、Cisco Secure Malware Analytics アプライアンスのソフトウェアスタックから完全に削除されました。以前の構成では、署名されていない構成ファイルをロードできませんでした（したがって、CVE-2020-10713 に対して脆弱ではありませんでした）が、新しいブートメカニズムは GRUB を完全に削除します。

手順

ステップ 1 **[操作（Operations）]** タブをクリックし、 **[電源（Power）]**を選択します。

図 *65 :* 電源



アプライアンスの電源が投入された日付が表示されます。

ステップ 2 **[再起動（Reboot）]** をクリックしてアプライアンスを再起動するか、**[シャットダウン（Shutdown）]** をクリックしてアプライアンスを完全にシャットオフします。

更新

『*Cisco Secure Malware Analytics Appliance Getting Started Guide*』に記載されている通り、Cisco Secure Malware Analytics アプライアンスを新しいバージョンに更新する前に、初期セットアップと構成手順を完了する必要があります。

（注） 新しい Cisco Secure Malware Analytics アプライアンスが古いバージョンのソフトウェアを搭載して出荷された場合、更新をインストールするには、まず初期設定を完了する必要があります。ライセンスがインストールされるまで更新はダウンロードされず、Cisco Secure Malware Analytics アプライアンスが完全に設定されない限り（データベースを含む）、正しく適用されない可能性があります。

新しい更新を確認して（**[操作（Operations）]** > **[更新（Update）]**）、それらを適用できます。

構成は、通常の起動プロセスの一部として実行されるようになりました。再起動のたびに、アプライアンスは完全に管理されたソフトウェア ロードアウトにリセットされます（実行時にコード署名がチェックされます）。以前は複数の再起動を伴う再設定サイクル中にのみ発生していた設定操作が、各起動サイクルの一部として発生するようになりました。したがって、次のようになります。

- 再インストール操作を伴う再設定は冗長になります。
- アップグレードのインストールが迅速になり、再起動は 1 回だけで済みます。

更新をインストールする際、次の点を考慮する必要があります。

- Cisco Secure Malware Analytics アプライアンスの更新は、管理 UI を介して適用されます。
- 更新サーバーが更新を送信すると、クライアントは更新後のバージョンに完全に移行します。暫定リリースをスキップすることが常に可能というわけではありません。スキップできない場合、更新サーバーは、次の更新をダウンロードする前に、アプライアンスにリリースをインストールするよう求めます。
- サーバーが特定のバージョンのダウンロードを許可する場合、そのバージョンに直接移行することができます。つまり、単一のアップグレードに必要な再起動以外の再起動を途中で求められることはありません。
- 更新は不可逆です。つまり、新しいバージョンにアップグレードした後、前のバージョンに戻すことはできません。
- オフライン(エアギャップ)更新プロセスについては、「Update Secure Malware Analytics Appliance」を参照してください。

バージョン ルックアップ テーブル

正しいビルド番号と対応するリリースバージョンを確認するには、「*Cisco Secure Malware Analytics アプライアンス バージョン ルックアップ テーブル*」を参照してください。

ポートの更新

Cisco Secure Malware Analytics アプライアンスはポート 22 を使用して SSH でリリース更新プログラムをダウンロードします。

- リリース更新は、Web ベースの管理インターフェイス（Admin UI）からだけではなく、テキスト（curses）インターフェイスからも適用できます。
- DHCP を使用するシステムでは、明示的に DNS を指定する必要があります。DNS サーバーが明示的に指定されていないシステムのアップグレードは失敗します。

データベーススキーマの更新

従来、スタンドアロンアプライアンスでは、システムがシングルユーザーモードでオフラインになっている間に、更新に関連したデータベース移行が発生しました（最初にアップグレードされたノードがオンラインに戻った後に更新が発生したクラスタは除きます。こうしたクラスタが例外になるのは、バックグラウンドで実行される可能性のある非常に長い更新が発生するためです。このような更新はケースバイケースで処理されました）。

Cisco Secure Malware Analytics アプライアンス（v2.5.0 以降）は、システムの再起動が完了した後にデータベーススキーマを更新します。そのため、起動プロセスの所要時間がやや長くなる場合があります。（非常に長い再起動は、引き続きケースバイケースで処理されます）。

以前のリリースでは、バックアップサポートが有効になっているクラスタ化されていないシステムは、NFS サーバーがダウンした場合、正常な動作をベストエフォートで試行していました。この動作は、Elasticsearch 機能の変更により、現在は保証できなくなっています。

v2.7.2 以降、ES6 ネイティブインデックスへのバックグラウンド Elasticsearch インデックスの移行が有効になりました。この移行は、Elasticsearch 7.0 以降が必要なバージョンの Cisco Secure Malware Analytics アプライアンスがインストールされる前に、正常に完了している必要があります。

（注） Elasticsearch インデックスの移行により、NFS バックアッププロセスに大幅な遅延が発生し、関連した警告が発生する可能性があります。インデックス移行がアクティブに進行中であることを示す場合、これらの警告は無視する必要があります。インデックス移行プロセスが長時間にわたって先に進まない場合は、サポート付きのチケットのみを生成する必要があります。

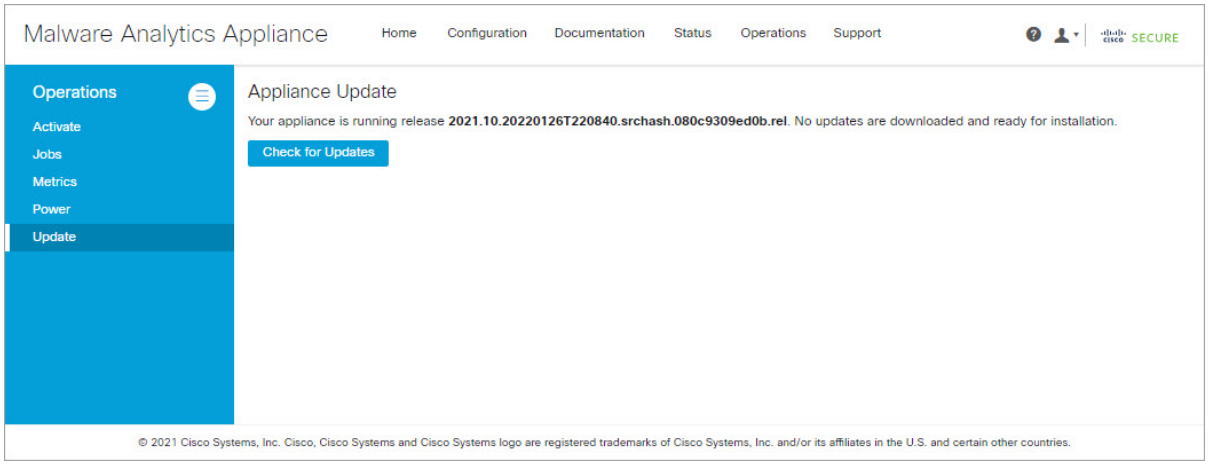
更新のインストール

更新を確認し、Cisco Secure Malware Analytics アプライアンスを更新するには、次の手順を実行します。

手順

ステップ 1 [操作（Operations）] タブをクリックし、[更新（Update）] を選択して [アプライアンスの更新（Appliance Updates）] ページを開きます。

図 *66* : アプライアンスの更新ページ



現在のリリースバージョンは、ページの上部に表示されます。また、インストール可能なアップデートがあるかどうかも通知されます。リリースバージョンについては、『*Cisco Secure Malware Analytics Appliance Version Lookup Table*』を参照してください。

ステップ 2 [更新の確認（Check for Updates）] をクリックします。

Cisco Secure Malware Analytics アプライアンスソフトウェアの最新の更新/バージョンがあるかどうかを確認するためのチェックが実行され、ある場合はダウンロードされます。これには少し時間がかかる場合があります。

ステップ 3 更新プログラムのダウンロードが完了したら、[更新を適用（Apply Update）] をクリックしてインストールします。

更新のトラブルシューティング

ここでは、アプライアンスの更新中に発生する可能性のある問題と、それらを解決する方法について説明します。

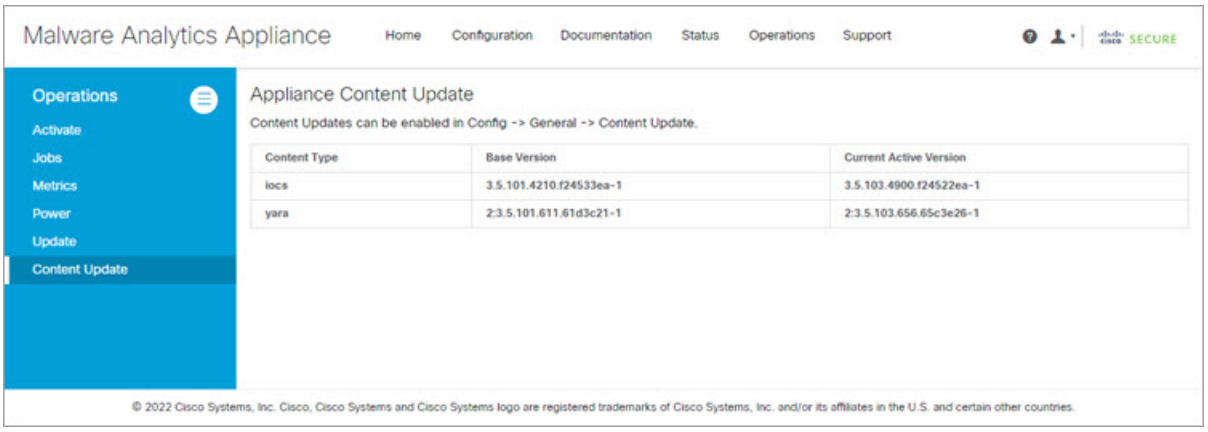
データベースの更新に失敗しました（Database Upgrade - Not Successful）メッセージ

「*database upgrade not successful*（データベースのアップグレードに失敗しました）」のメッセージは、新しい Secure Malware Analytics アプライアンスが古いバージョンの PostgreSQL を実行しており、データベースの自動移行プロセスに失敗した場合に表示されることがあります。v2.0 へのアップグレードの前に、この状態を修正することが必要です。詳細については、『*Cisco Threat Grid Appliance Release Notes v2.0.1*』を参照してください。

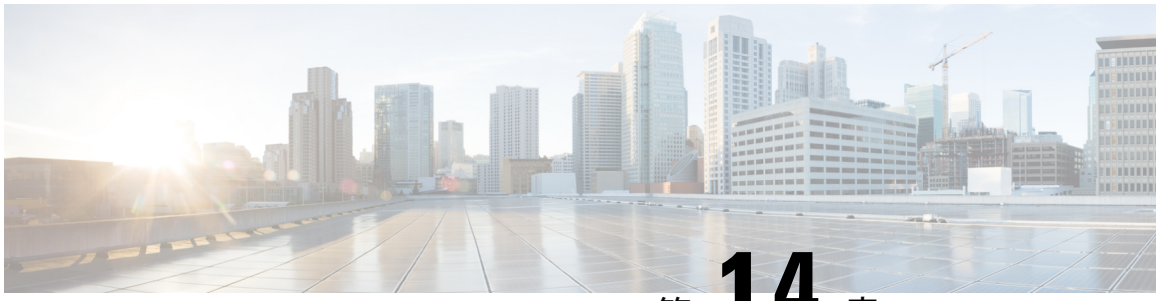
アプライアンス コンテンツの更新

[アプライアンスコンテンツの更新（Appliance Content Update）] ページは、侵入兆候、または iocs（侵害指標）と yara の基本バージョンと最新バージョンを提供します。

図 *67*：アプライアンス コンテンツの更新



（注） アプライアンスを更新している間に、アプライアンスを最新の *iocs* および *yara* に更新します。アプライアンスの詳細については、「更新 （138 ページ）」を参照してください。



第 14 章

サポート

この章では、Cisco Secure Malware Analytics アプライアンスの問題の解決を支援するために、サポートセッションを開始し、サポートスナップショットを取得する手順について説明します。

サポート ケースを開く

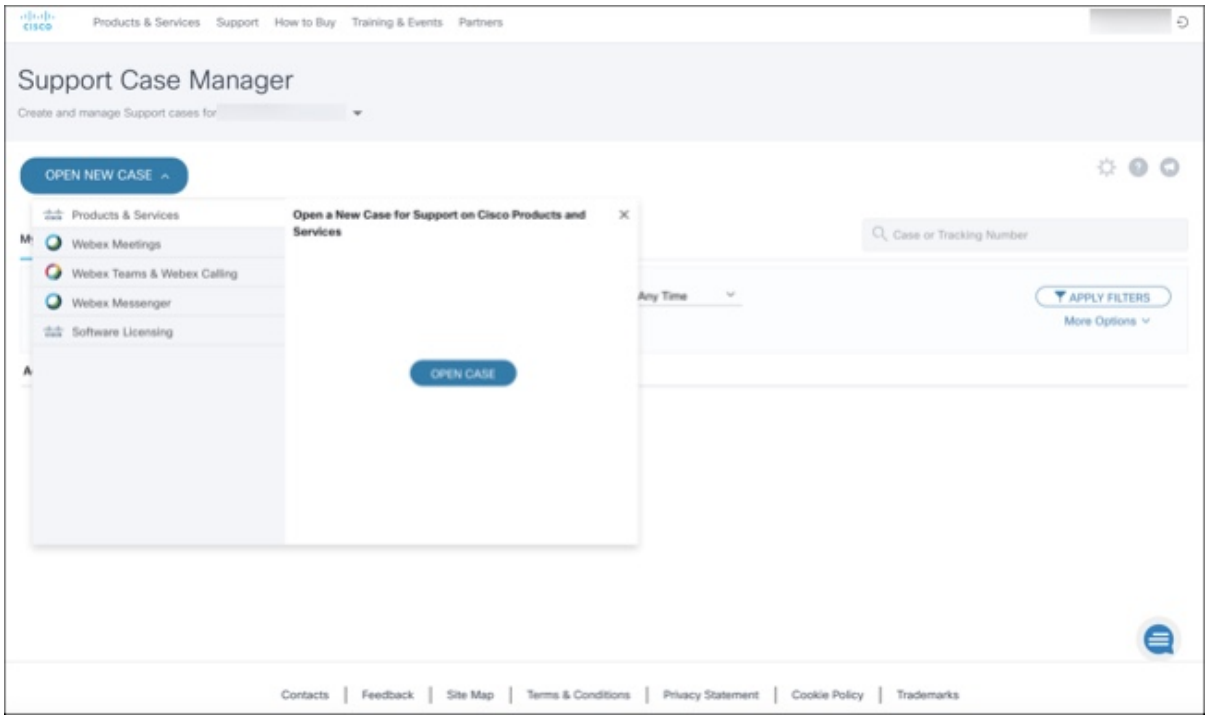
Cisco Secure Malware Analytics に関するご質問やサポートについては、https://mycase.cloudapps.cisco.com/case でサポート ケース マネージャをオープンしてください。

（注） Cisco Secure Malware Analytics のエンジニアからサポートを受ける場合、アプライアンスへのリモートアクセスが必要な場合があります。ライブ サポート セッションを開始する方法、およびアプライアンスのスナップショットを取得する方法の詳細については、ライブ サポート セッションの開始 を参照してください。

手順

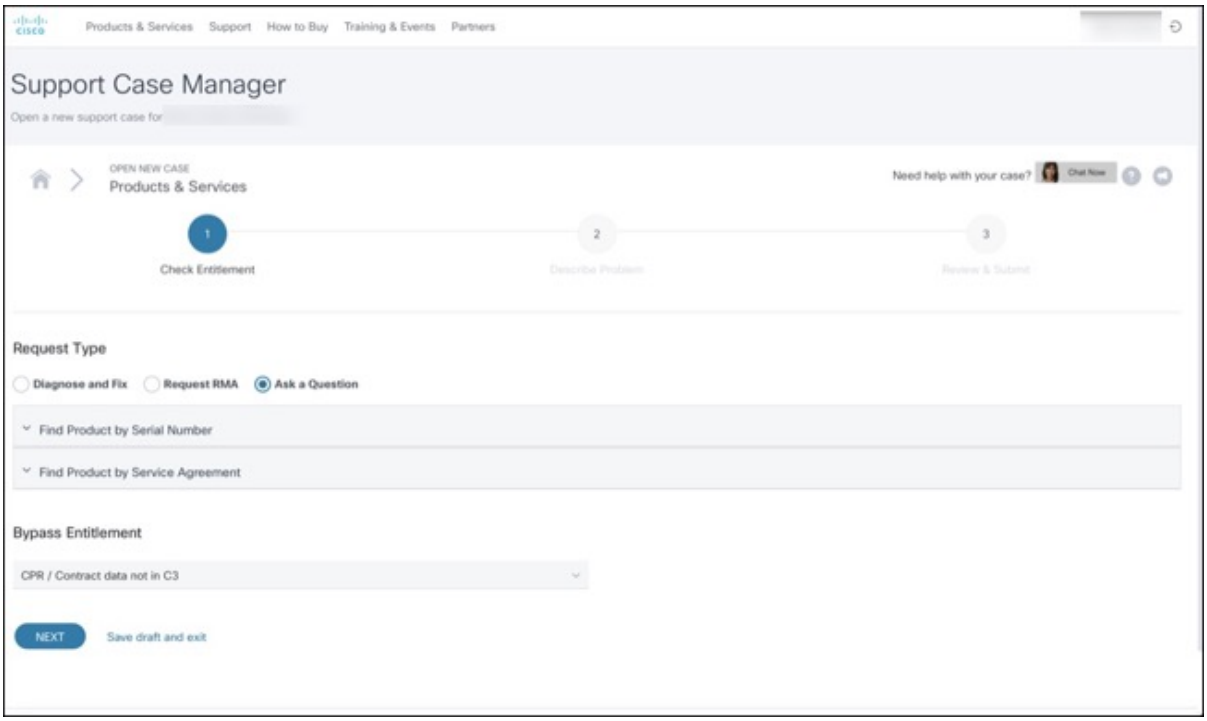
ステップ 1 Support Case Manager で、**[Open New Case] > [Open Case]** をクリックします。

図 *68 :* 新しいケースをオープンする



ステップ 2 [**Ask a Question**] オプションボタンをクリックし、使用中のシスコセキュリティ**製品シリアル番号**または**製品サービス契約**を検索します。検索の対象は、Cisco Secure Malware Analytics のシリアル番号またはサービス契約である必要があります。

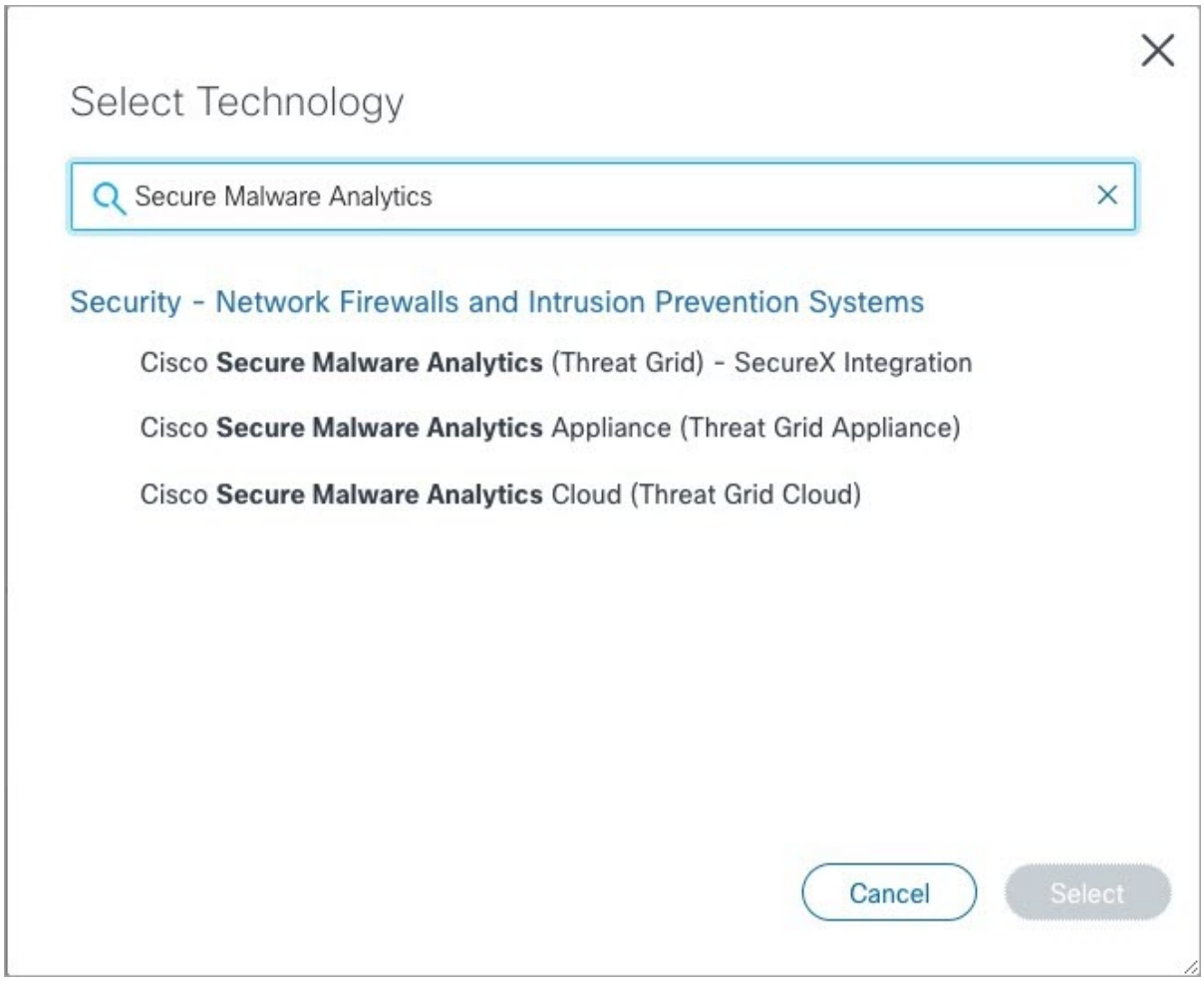
図 *69* : エンタイトルメントのチェック



ステップ 3 **[問題の説明（Describe Problem）]** ページで、問題の **[タイトル（Title）]** と **[説明（Description）]** (タイトルに Cisco Secure Malware Analytics と記載）を入力します。

ステップ 4 [テクノロジーを手動で選択（Manually Select A Technology）] をクリックして、[Cisco Secure Malware Analytics] を検索します。

図 *70* : テクノロジーの選択



ステップ 5 リストから [Cisco Secure Malware Analyticsアプライアンス（Cisco Secure Malware Analytics Appliance）] を選択し、[選択（Select）] をクリックします。

ステップ 6 フォームの残りの部分をすべて入力し、[**Submit**] をクリックします。

ケースをオンラインで開くことができない場合は、シスコサポートにお問い合わせください。

- **米国およびカナダ**：1-800-553-2447
- **各国の連絡先**：https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

サポートを依頼する方法の詳細については、以下を参照してください。

- 次のブログ記事を参照してください。『**Changes to the Cisco Secure Malware Analytics Support Experience**』（https://community.cisco.com/t5/security-blogs/changes-to-the-cisco-threat-grid-support-experience/ba-p/3911407）

- https://www.cisco.com/c/en/us/support/index.html で**シスコサポート & ダウンロード**のメインページを参照してください。

ライブ サポート セッション

Cisco Secure Malware Analytics のエンジニアからのサポートを必要とする場合、「サポート モード」を有効にするよう求められる場合があります。このモードは、ライブ サポート セッションであり、Secure Malware Analytics サポート エンジニアにアプライアンスへのリモートのアクセス権を付与します。アプライアンスの通常の動作は影響を受けません。ライブ サポート セッションは、**[ライブ サポート セッション（Live Support Session）]** ページから開始できます。

（注） また、リカバリモードでの起動時にAdmin TUIからサポートモードを有効にすることもできます（手順については、 管理者パスワードのリセットを 参照してください）。

サポート サーバ

サポート セッションを確立するには、アプライアンスが次のサーバに到達する必要があります。

- **support-snapshots.threatgrid.com** ：これにより、Cisco のサポートスタッフにアプライアンスへの直接アクセス権を与えたり、ファイルをダウンロードしてそのファイルをアップロード/サポートチケットに添付したりする必要なく、サポート用のスナップショットを直接アップロードできます。
- **rash.threatgrid.com** ：このサポート モードでは、Cisco のサポート スタッフがログインしてアプライアンスを直接検査できます。

アクティブなサポートセッション中のファイアウォールでは、両方のサーバが許可されている必要があります。Cisco Secure Malware Analytics アプライアンスのインターフェイスごとに推奨されるファイアウォール ルールの詳細については、「SMA ファイアウォール ルール」を参照してください。

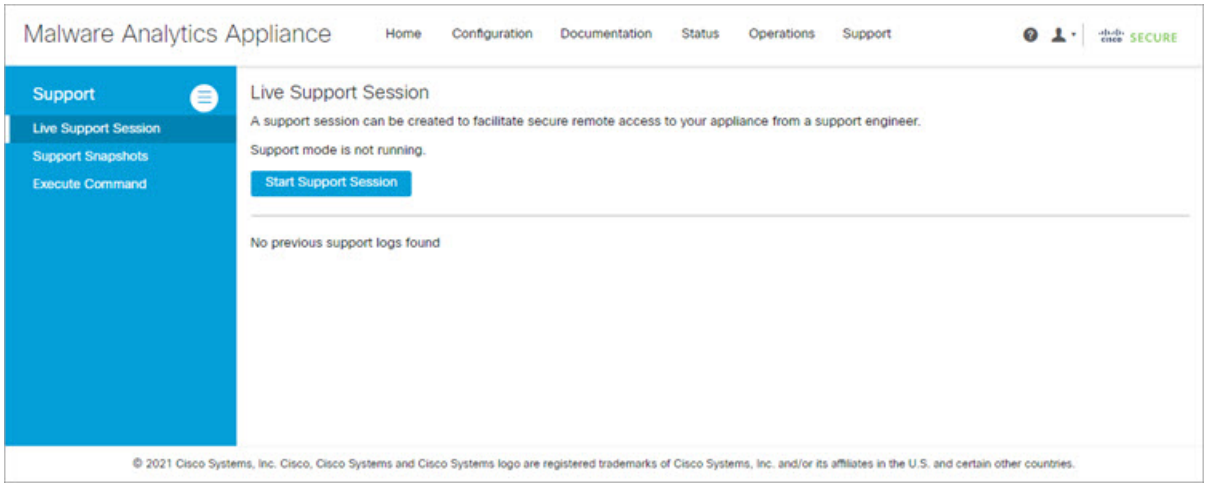
ライブ サポート セッションの開始

ライブ サポート セッションは、**[ライブサポートセッション（Live Support Session）]** ページから開始できます。

手順

ステップ 1 **[サポート（Support）]** メニューをクリックして、**[ライブ サポート セッション（Live Support Session）]** を選択します。

図 *71* : ライブ サポート セッション



ステップ 2 **[サポートセッションの開始（Start Support Session）]** をクリックして、プロンプトに従います。

ステップ 3 セッションを終了するには、**[サポートセッションの終了（Terminate Support Session）]** をクリックします。

サポート スナップショット

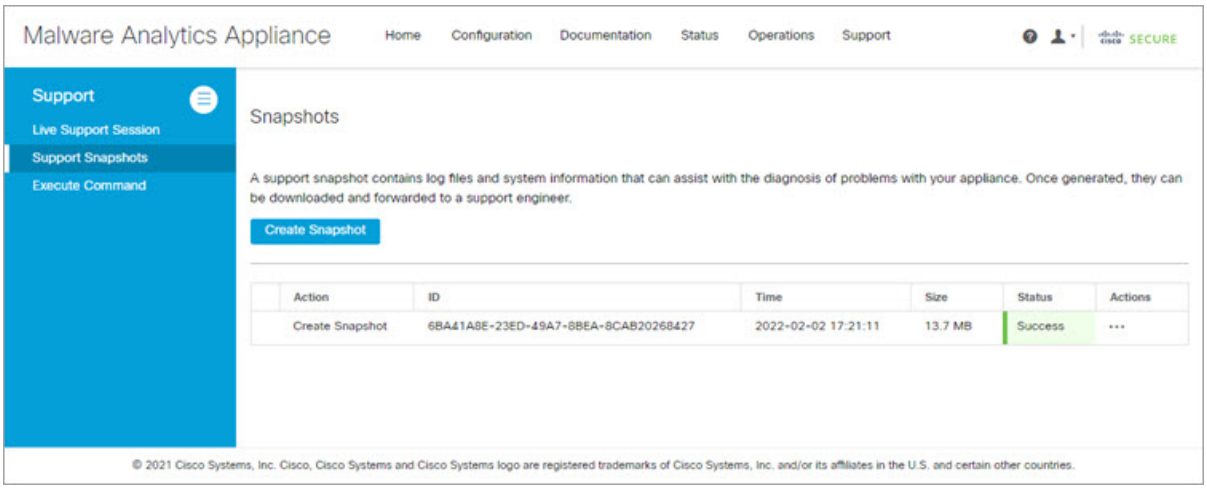
サポートスナップショットは、基本的に実行中のシステムのスナップショットで、ログ、psoutput などが含まれており、サポートスタッフによる問題のトラブルシューティングに役立ちます。

（注） v2.11 更新より前に取得したスナップショットのコンテンツが表示または送信できなくなる場合があります。

手順

ステップ 1 スナップショットを取得するには、**[サポート（Support）]** タブをクリックし、[サポート（Support）] **[スナップショット（Snapshots）]**を選択します。

図 *72 :* サポート スナップショット



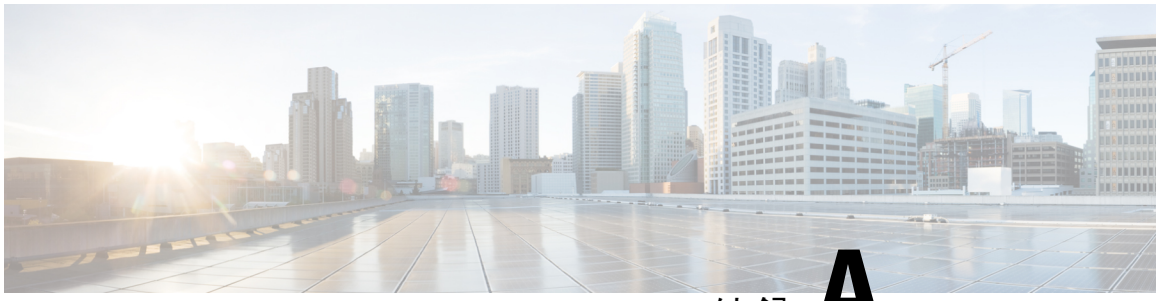
ステップ 2 「**スナップショットの作成**」をクリックします。スナップショットが取得され、ページに追加されます。

ステップ 3 スナップショットを取得したら、ジョブの詳細を表示でき、**.tar** ファイル ファイルとしてダウンロードするか、**[送信（Submit）]** をクリックして、スナップショットを Cisco Secure Malware Analytics スナップショット サーバに自動的にアップロードします。

スナップショットを削除するには、 **[削除（Delete）]**をクリックします。

スナップショットを使用してバックアップを確認する

また、スナップショットを使用して、バックアップが適切かどうかをテストおよび検証することもできます。実稼働アプライアンスまたはクラスタのバックアップストアのスナップショットをとり、そこから新しい書き込み可能なボリュームを作成して、そのスナップショットから非実稼働アプライアンスまたはクラスタの復元を試みます。



付録 A

組織およびユーザー

Cisco Secure Malware Analytics は、デフォルトの組織および管理者ユーザーを使用して Cisco Secure Malware Analytics アプライアンスにインストールされます。セットアップとネットワーク設定が完了したら、ユーザーがログインして分析用のマルウェアサンプルの送信を開始できるように、追加の組織とユーザーアカウントを作成できます。

組織の構成によっては、組織、ユーザー、管理者を追加する際に複数のユーザーやチーム間での計画と調整が必要になる場合があります。この章では、Cisco Secure Malware Analytics で組織とユーザーを管理する方法について説明します。内容は次のとおりです。

新規組織の作成

ユーザーは常に特定の組織と関係しています。ユーザーを追加する前に、まず組織を作成して、その組織にユーザーを追加できるようにする必要があります。新しい組織を作成するには、管理者としてログインする必要があります。これは、Cisco Secure Malware Analytics ポータル UI の **[組織の管理（Managing Organizations）]** ページで実行します。

重要 一度作成された組織をインターフェイスから削除することはできないため、このタスクは慎重に計画する必要があります。

手順

ステップ 1 Cisco Secure Malware Analytics ポータルに管理者としてログインします。

ステップ 2 **[管理（Administration）]** メニューをクリックし、**[組織の管理（Manage Organization）]** を選択します。**[組織（Organizations）]** ページが開き、アプライアンスで設定されているすべての組織が表示されます。

組織およびユーザー

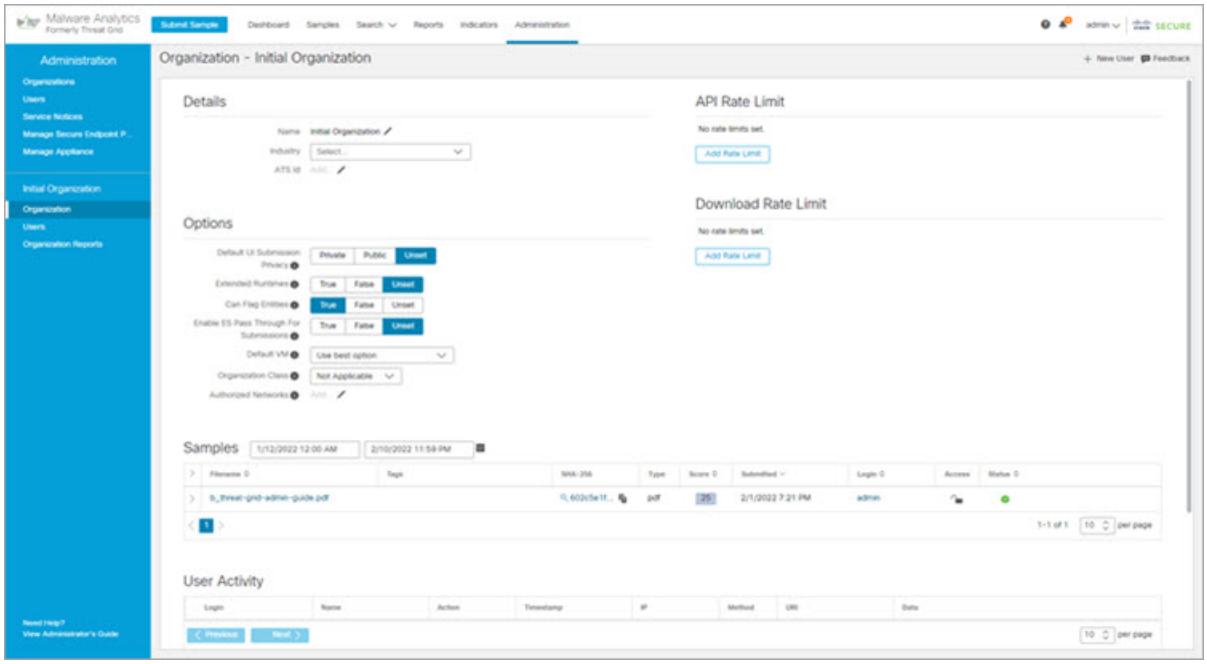
ステップ 3 ページの右上隅にある **[新しい組織（New organization）]** をクリックして、**[新しい組織（New organization）]** ダイアログを開きます。

ステップ 4 以下の項目に入力します。

- [**Name**]：組織の名前を入力します（現在、名前にサイズ制限はありません）。
- **業界（Industry）** - **[業界（Industry）]** ドロップダウン リストからビジネスのタイプを選択します。該当する業界がリストにない場合は、[**Unknown**] に設定したままにし、Cisco Secure Malware Analytics サポート ケースを開くに連絡してオプションの追加を依頼してください。
- [**ATS ID**]：高度な脅威サービス ID を入力します。

ステップ 5 [**送信 (Submit)**] をクリックします。新しい組織が作成され、[Organizations] リストに表示されます。

図 *73* : デフォルトの初期組織の組織ページ



ステップ 6 新しく作成した組織を編集し、次の情報を入力します。

- [**Options**]：必要に応じて入力します。
- [**Rate Limit**]：デフォルトのユーザー送信レート制限を設定します。

  API レート制限は、ライセンス契約条件に基づいて Cisco Secure Malware Analytics アプライアンス全体に適用されます。この制限は、API送信のみに適用され、手動でのサンプル送信には適用されません。ライセンスのレート制限は、組織に適用されます。

  Cisco Secure Malware Analytics ポータルのオンラインヘルプに記載されているように、個々のユーザーにサンプル送信レートを設定することもできます。

  レート制限は、暦日ではなく、24 時間単位の時間枠に基づきます。送信レートの上限に達すると、次の API 送信で、429 エラーと、再試行までの待機時間を示すメッセージが返されます。

組織が作成されると、管理者または組織の管理者がそれを管理できます。

ユーザーの管理

ユーザーの追加方法など、ユーザーアカウントの作成と管理に関する手順とマニュアルについては、Cisco Secure Malware Analytics Portal UI のオンラインヘルプを参照してください。

ナビゲーション バーで、**[ヘルプ（Help）] > [Cisco Secure Malware Analytics オンライン ヘルプの使用（Using Secure Malware Analytics Online Help）] > [Cisco Secure Malware Analytics ユーザーの管理（Managing Secure Malware Analytics Users）]** をクリックします。

（注） ユーザーは、API のみで削除でき、サンプルを送信していない場合にのみ削除できます。

E メール セキュリティ アプライアンス、Web セキュリティ アプライアンスなどのデバイスを統合するためのデバイス ユーザー アカウントの管理については、「新しいデバイスユーザーアカウントの有効化」を参照してください。

組織とユーザーの削除

組織とユーザーは、管理者ユーザーが Cisco Secure Malware Analytics API を使用して削除できます。組織は、ユーザーがいない場合にのみ削除できます。ユーザーが含まれている場合は、組織を削除する前にユーザーを削除する必要があります。ただし、サンプルを送信していない場合にのみユーザーを削除できます。

- 組織を削除するには、Cisco Secure Malware Analytics API（/api/v3/organizations/:org-id）と DELETE を使用します。
- ユーザーを削除するには、Cisco Secure Malware Analytics API（/api/v3/users/:user-id）と DELETE を使用します。

API エンドポイントの詳細については、Cisco Secure Malware Analytics ポータルのオンラインヘルプを参照してください。

新しいデバイスユーザーアカウントの有効化

Cisco Email Security アプライアンス、Web Security アプライアンス、または他の Cisco Sandbox API 統合が Cisco Secure Malware Analytics アプライアンスに接続して登録されると、新しい Cisco Secure Malware Analytics ユーザーアカウントが自動的に作成されます。ユーザーアカウントの初期ステータスは、非アクティブになっています。Cisco Secure Malware Analytics アプ

組織およびユーザー

ライアンス管理者は、分析用のマルウェアサンプルの送信に使用する前に、デバイスユーザーアカウントを手動でアクティブにする必要があります。

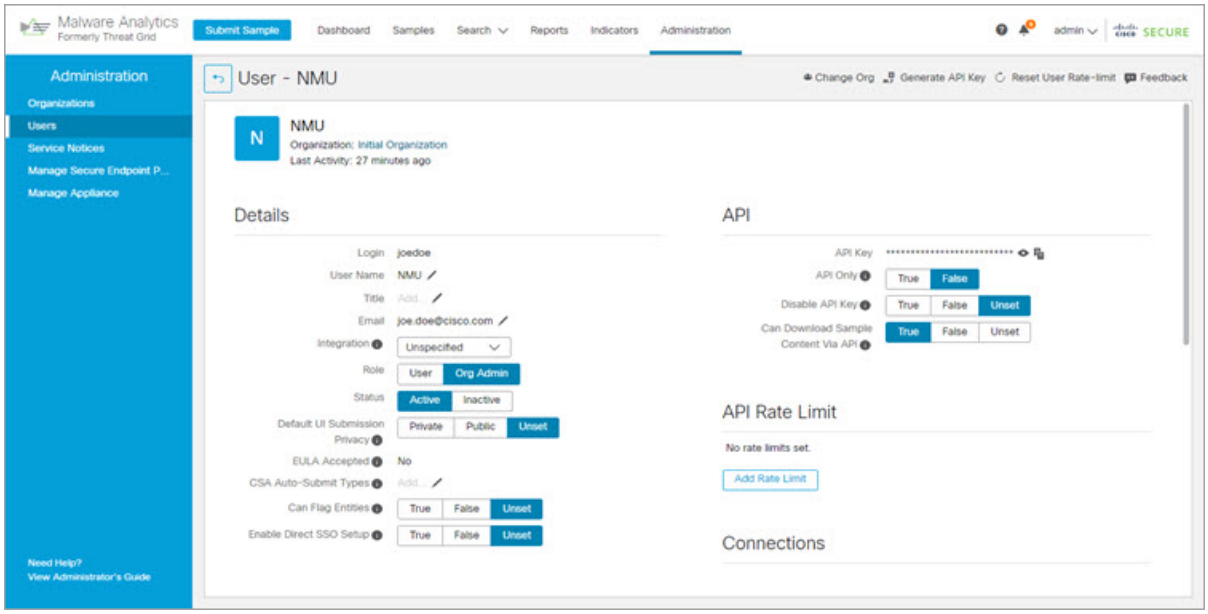
手順

ステップ 1 Cisco Secure Malware Analytics ポータル UI に管理者としてログインします。

ステップ 2 **[管理（Administration）]** メニューをクリックし、**[ユーザーの管理（Manage Users）]** を選択します。

ステップ 3 デバイスのユーザーアカウントを見つけて、[**User Details**] ページを開きます。

図 *74*：ユーザの詳細

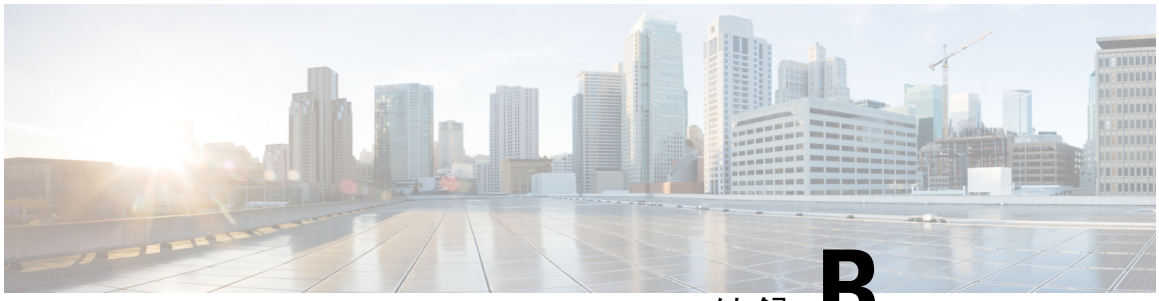


ユーザー ステータスは現在 **非アクティブ**です。

ステップ 4 [Activate] をクリックします。

ステップ 5 確認ダイアログで、アクションを確認します。

これで、統合するアプライアンスまたはデバイスが Cisco Secure Malware Analytics アプライアンスと通信できるようになります。



付録 B

インバウンドおよびアウトバウンド接続

インバウンド接続およびアウトバウンド接続を使用して、他のシスコのアプライアンス、デバイス、およびサービスと通信するように Cisco Secure Malware Analytics アプライアンスを設定できます。暗号化された SSL 接続により、他のアプライアンス（E メール セキュリティ アプライアンスや Web セキュリティアプライアンスなど）が、分析のために潜在的なマルウェアサンプルを Cisco Secure Malware Analytics に送信できるようになります（インバウンド接続）。

また、アウトバウンド接続を介して、配置更新サービスのために Cisco Secure Endpoint プライベートクラウドと通信するように Cisco Secure Malware Analytics アプライアンスを設定できます。

この付録では、インバウンド接続とアウトバウンド接続の両方を設定する手順について説明します。

ESA または WSA の Secure Malware Analytics アプライアンスへの接続

Cisco Secure Malware Analytics アプライアンスと Cisco E メール セキュリティ アプライアンス（ESA）または Web セキュリティアプライアンス（WSA）間の接続は、Cisco Sandbox API（CSA API）によって有効になり、CSA 統合と呼ばれることがよくあります。ESA/WSA アプライアンスは、分析用のサンプルを送信する前に、Secure Malware Analytics アプライアンスに登録する必要があります。

ESA/WSA を Secure Malware Analytics アプライアンスに登録するには、まず ESA/WSA の管理者が、使用中のアプライアンスとネットワーク環境に適した SSL 証明書接続をセットアップする必要があります。

インバウンドおよびアウトバウンド接続

ESA/WSA のマニュアル

ESA/WSA の製品マニュアルで、「Enabling and Configuring File Reputation and Analysis Services」の手順を参照してください。

- 『*Cisco Email Security Appliance User Guides*』
- 『*Cisco Web Security Appliance User Guides*』

（注） これらのマニュアルで、Secure Malware Analytics アプライアンスは、多くの場合「分析サービス」または「プライベートクラウドファイル分析サーバー」と呼ばれています。

インバウンド接続の概要

インバウンド接続を設定する場合、次の作業を実行する必要があります。

（注） Cisco Secure Malware Analyticsは、クラスタまたはスタンドアロンSMAアプライアンスのいずれかと通信できる1つの環境とのみ通信できます。環境がクラスタの場合は、クラスタ内のすべてのノードを追加する必要があります。

- **SSL 証明書のセットアップ**：Secure Malware Analytics アプライアンスの SSL 証明書の SAN（サブジェクト代替名）または CN（共通名）は、ホスト名および ESA/WSA の想定と一致している必要があります。統合先の ESA/WSA との接続を成功させるには、統合先の ESA/WSA が Secure Malware Analytics アプライアンスの識別に使用するものと同じホスト名にする必要があります。

  要件に応じて、Secure Malware Analytics アプライアンスで自己署名 SSL 証明書を再生成する必要があります。その際、[SAN/CN] フィールドには現在のホスト名が入力されます。この証明書を作業環境にダウンロードし、統合先の ESA/WSA にアップロードしてインストールできます。

  あるいは、企業向けの SSL 証明書や市販の SSL 証明書（または手動で生成した証明書）をアップロードして、現在の Secure Malware Analytics アプライアンスの SSL 証明書と置き換えなければならないこともあります。詳細な手順については、SSL 証明書の置き換え（77 ページ）を参照してください。

- **接続性の確認**：SSL 証明書の設定が完了したら、次の手順として、ESA/WSA が Secure Malware Analytics アプライアンスと通信できることを確認します。ESA/WSA は、ネットワーク経由で Secure Malware Analytics アプライアンスのクリーン インターフェイスに接続できる必要があります。製品マニュアルの手順に従って、Secure Malware Analytics アプライアンスと ESA/WSA が相互に通信できることを確認します（ESA または WSA の Secure Malware Analytics アプライアンスへの接続を参照）。

- **ESA/WSA ファイル分析の構成の完了**：**ファイル分析セキュリティ** サービスを有効にし、詳細を構成します。

- **Cisco Secure Malware Analytics アプライアンスへの ESA/WSA の登録** ：製品マニュアルに従って設定された ESA/WSA は、Cisco Secure Malware Analytics アプライアンスに自動的に登録されます。接続先デバイスの登録時に、デバイス ID がログイン ID となる新しい Cisco Secure Malware Analytics ユーザーが自動的に作成され、同じ ID に基づく名前を使用して新しい組織が作成されます。管理者は、新しいデバイスユーザーアカウントをアクティブにする必要があります。
- **Cisco Secure Malware Analytics アプライアンスでの新しい ESA/WSA アカウントのアクティブ化** ：ESA/WSA または他の統合が接続され、それ自体が Cisco Secure Malware Analytics アプライアンスに登録されると、新しい Cisco Secure Malware Analytics ユーザー アカウントが自動的に作成されます。ユーザーアカウントの初期ステータスは、非アクティブになっています。Cisco Secure Malware Analytics アプライアンス管理者は、分析用のマルウェア サンプルの送信に使用する前に、デバイス ユーザー アカウントを手動でアクティブにする必要があります。

インバウンド接続の構成

ESA/WSA 間の接続は、Cisco Secure Malware Analytics アプライアンスから見れば受信になり、CSA API を使用します。

（注） 実行する必要のあるタスクの詳細については、ESA および WSA 製品のマニュアルを参照してください。

手順

ステップ 1 Cisco Secure Malware Analytics アプライアンスを通常どおりに（まだ統合されていない状態で）セットアップして構成します。

ステップ 2 更新を確認し、必要に応じてインストールします。

ステップ 3 ESA/WSA を通常どおりに（まだ統合されていない状態で）セットアップして設定します。

ステップ 4 Cisco Secure Malware Analytics アプライアンス SSL 証明書 SAN または CN は、現在のホスト名と ESA/WSA の想定と一致する必要があります。自己署名 SSL 証明書を展開する場合は、（Cisco Secure Malware Analytics アプリケーションのクリーンインターフェイスで）新しい SSL 証明書を生成し、必要に応じてデフォルトと置き換え、ダウンロードして ESA/WSA にインストールします（「SSL 証明書の置き換え」を参照）。

（注）
Cisco Secure Malware Analytics アプライアンスのホスト名が SAN または CN になっている証明書を生成してください（Cisco Secure Malware Analytics アプライアンスのデフォルトの証明書は機能しません）。IP アドレスではなく、ホスト名を使用します。

ステップ 5 ESA/WSA は、ネットワーク経由で Secure Malware Analytics アプライアンスのクリーン インターフェイスに接続できることを確認します。

ステップ 6 Cisco Secure Malware Analytics アプライアンスとの統合用に ESA/WSA を構成します。詳細な手順については、ESA/WSA 製品のマニュアルを参照してください。

ステップ 7 変更を送信し、保存します。

Cisco Secure Malware Analytics アプライアンスへの ESA/WSA の登録は、ファイル分析の設定を送信すると自動的に実行されます。

ステップ 8 Cisco Secure Malware Analytics アプライアンスで新しいデバイスユーザーアカウントをアクティブ化します。

a) Cisco Secure Malware Analytics ポータル UI に管理者としてログインします。
b) **[管理（Administration）**] タブをクリックし、 **[ユーザーの管理（Manage Users）]** を選択して [**ユーザー（Users）]** ページを開きます。
c) ユーザー名をクリックして、デバイス ユーザ アカウントの [ユーザーの詳細（User Details）] ページを開きます（探すために検索を使用する必要がある場合があります）。
d) ユーザー ステータスは現在 **非アクティブ**です。 **[現用系（Active）]** をクリックして、新しいアカウントをアクティブ化します。
e) 確認ダイアログで、アクションを確認します。

ESA/WSA は、Cisco Secure Malware Analytics アプライアンスとの接続を開始できるようになりました。

Cisco Secure Endpoint プライベートクラウドを Cisco Secure Malware Analytics アプライアンスに接続

Cisco Secure Malware Analytics アプライアンスは、配置更新サービス用の Cisco Secure Endpoint プライベートクラウドとの統合をアウトバウンド接続としてサポートします。

（注） 特に新しいアプライアンスを設定する場合は、Cisco Secure Malware Analytics アプライアンス配置更新サービスと Cisco Secure Endpoint プライベートクラウドの統合の設定タスクを、指定された順序に従ってデバイスで実行する必要があります。すでにセットアップして設定されているアプライアンスを統合する場合は、順序はそれほど重要ではありません。

実行するタスクの詳細については、Cisco Secure Endpoint プライベートクラウドのマニュアルを参照してください。

手順

ステップ 1 Cisco Secure Malware Analytics アプライアンスを通常どおりに（まだ統合されていない状態で）セットアップして設定します。更新を確認し、必要に応じてインストールします。

ステップ 2 Cisco Secure Endpoints プライベートクラウドを通常どおりに（まだ統合されていない状態で）セットアップして設定します。

ステップ 3 Cisco Secure Malware Analytics アプライアンス管理 UI で、**[設定（Configuration）]** タブをクリックし、**[SSL]**を選択します。

ステップ 4 必要に応じて、クリーンインターフェイスで SSL 証明書を再生成してデフォルトの証明書を置き換え、そのコピーを作成して Cisco Secure Endpoint プライベートクラウド デバイスにインストールする（詳細については、 SSL 証明書の再生成 を参照）。

ステップ 5 Cisco Secure Endpoint プライベート クラウド デバイスで統合を設定するために必要な次の情報を取得します。

- **ホスト名**：**[Configuration] > [Hostname]** をクリックし、ホスト名をメモします。
- **API キー**：Cisco Secure Malware Analytics ポータルの **[ユーザーの詳細（User Details）]** ページから **API キー** をコピーします（**[管理（Administration）]** タブをクリックし、[ユーザーの **管理（Manage Users**）] を選択してから、統合ユーザーアカウントに移動して、 **[ユーザーの詳細（User Details）]** ページで API キーを見つけます）。

  （注）
  この手順を実行するには管理者ユーザーでなければならないというわけではありません。Cisco Secure Malware Analytics アプライアンスで、この目的のために特別にユーザーを作成することも可能です。

ステップ 6 Cisco Secure Malware Analytics アプライアンスとの統合用に Cisco Secure Endpoint プライベート クラウド デバイスを設定する。詳細な手順については、ESA/WSA 製品のマニュアルを参照してください。この設定により、AMP が Cisco Secure Malware Analytics アプライアンスと通信できるようになります。これで、Cisco Secure Malware Analytics にサンプルを送信できるようになりました。

ステップ 7 残りの手順を実行して、処理結果を Cisco Secure Malware Analytics アプライアンスに通知するように廃棄更新サービスを設定します（詳細については、「Secure Endpoint プライベートクラウド」のユーザーマニュアルを参照してください）。

a) 必要に応じて、DNS を設定します。「DNS の設定」を参照してください。
b) 統合先のデバイスを信頼できるように、Cisco Secure Endpoint プライベートクラウド SSL 証明書を Cisco Secure Endpoint アプライアンスにダウンロードするかコピーして貼り付けます。「CA 証明書」を参照してください。
c) Cisco Secure Malware Analytics ポータル UI で、AMP 処理更新サービスの URL とログイン情報を指定し、**[追加（Add）]** をクリックします（ 配置更新の配信サービスの管理」を参照）。

配置更新の配信サービスの管理

Cisco Secure Malware Analytics ポータルで、Cisco Secure Endpoint Private Cloud アプライアンス統合の Disposition Update Syndication Service を管理できます。URL は、[**Disposition Update Syndication Service**] ページで追加、編集、削除できます。

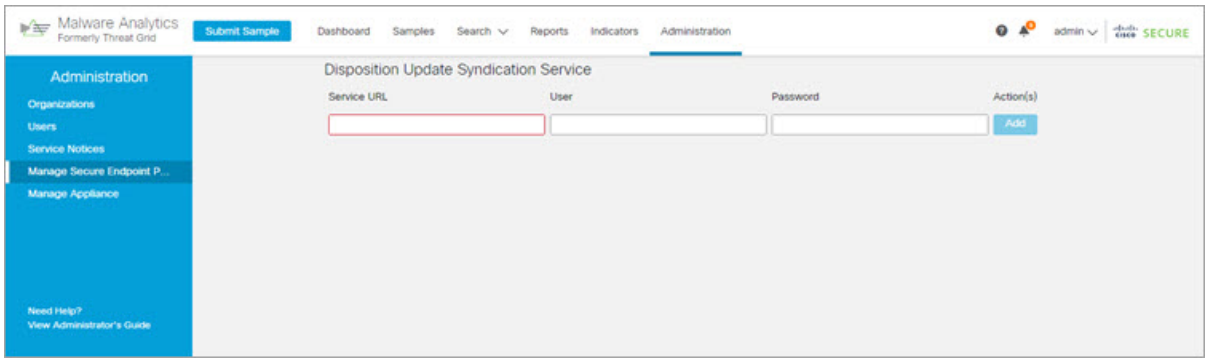
インバウンドおよびアウトバウンド接続

（注） Cisco Secure Endpoint プライベートクラウド アプライアンス統合の詳細については、 Cisco Secure Endpoint プライベート クラウドを Cisco Secure Malware Analytics アプライアンスに接続 を参照してください。

手順

ステップ 1 Cisco Secure Malware Analytics ポータルで、**[管理（Administration）]** タブをクリックし、**[Secure Endpoint プライベートクラウドとの統合の管理（Manage Secure Endpoint Private Cloud Integration）]** を選択して **[Disposition Update Syndication Service]** ページを開きます。

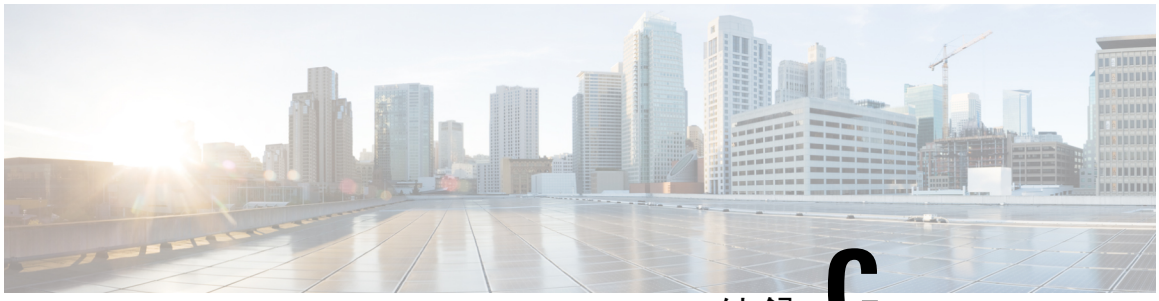
図 *75 :* 配置更新の配信サービス



ステップ 2 次の情報を入力します。

- **Service URL** - Cisco Secure Endpoint プライベート クラウド URL。
- **[User]**：管理者ユーザー名。
- **パスワード** - Cisco Secure Endpoint 構成ポータルにより提供されたパスワード。

ステップ 3 **[追加（Add）]** をクリックします。



付録 C

アプライアンスのワイプ操作によるすべてのデータの削除

この付録では、アプライアンスのワイプ操作を使用して、Cisco Secure Malware Analytics アプライアンスからすべてのデータを削除する方法について説明します。説明する項目は次のとおりです：

アプライアンスのワイプの概要

アプライアンスのワイプブートオプションを使用すると、Cisco Secure Malware Analytics アプライアンスのディスクをワイプして、廃棄前にすべてのデータを削除したり、Cisco Demo Loan Program に戻したりすることができます。

（注） [アプライアンスのワイプ（Wipe）] アプライアンス ブート オプションは、データのリセットと混同しないでください。[データ リセット（Data Reset）] は、 `destroy-data` コマンドでオペレーティング システム ログおよびその他の状態をクリアして、バックアップを復元するための準備を行います。

重要 アプライアンスのワイプ手順を実行すると、Cisco Secure Malware Analytics アプライアンスは、シスコに返却してイメージを再作成しない限り稼働しなくなります。

アプライアンスのワイプ手順

この操作は、管理 TUI から開始された tgsh ではなく、リカバリモードの tgsh でのみ使用できます。アプライアンスからのすべてのデータをワイプするには、次の手順を実行します。

手順

ステップ 1 アプライアンスを再起動します（**[操作（Operations）**] タブをクリックし、**[電源（Power）]**を選択してから [再 **起動（Reboot）**] ボタンをクリックします）。

ステップ 2 可能なブートターゲットのリストを表示するには [BIOS] ウィンドウで **F6** を押し、**[リカバリ（Recovery）]** を選択します。

Cisco Secure Malware Analytics シェルがリカバリモードで開きます。（「管理者パスワードのリセット」の図 6 を参照）

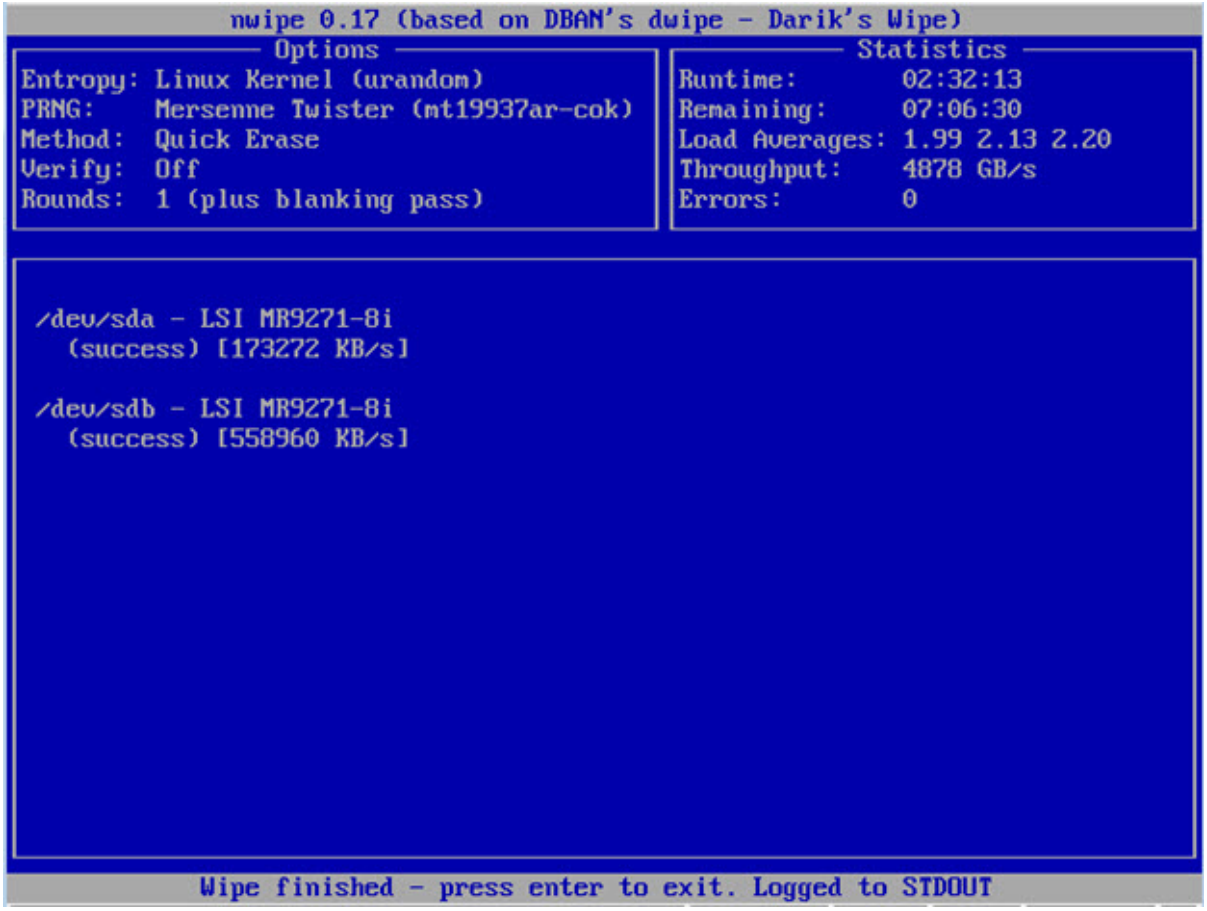
ステップ 3 リカバリモード tgsh で次のいずれかのコマンドを実行します。これらは、パフォーマンスと（理論的には）セキュリティのレベルのみで異なります（ただし、最新のドライブでは、高速メカニズムでも非常に優れたセキュリティを提供する可能性があります）。

- service start wipe-fast
- service start wipe-random
- service start wipe-3pass

これらのコマンドのいずれかを実行した直後に、ワイププロセスが開始されます。

ワイプ操作が完了すると、[**Wipe Finished**] ウィンドウが表示されます。

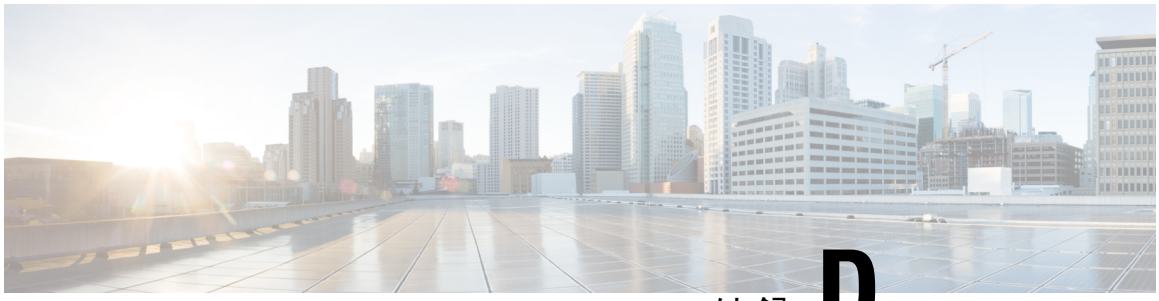
図 *76 : [Wipe Finished]*



ステップ 4 Enter を押して終了します。

Wipe アプライアンスおよびクラスタ

ワイプ操作を実行すると、Secure Malware Analytics アプライアンスは、シスコに返却してイメージを再作成しない限り稼働しなくなります。クラスタノードのワイプは、完全に削除されるというフラグが Admin UI でそのノードに付けられた後にのみ実行する必要があります。



付録 D

FirmwareUp によるファームウェアの更新

このトピックでは、**[ブート（Boot）]** メニューで使用可能な **[FirmwareUp]** オプションを使用してファームウェアを更新する方法について説明します。

ファームウェアの更新について

ファームウェアの更新は 、Cisco Secure Malware Analytics アプライアンスの最適なパフォーマンス、セキュリティ、および互換性を維持するために不可欠です。これらのアップデートでは、デバイスがベスト状態で動作するように、新機能、バグ修正、およびセキュリティ強化を導入することがよくあります。

ファームウェアの更新手順

始める前に

Cisco Secure Malware Analytics アプライアンスのバージョンが 2.19.4 以降であることを確認します。

手順

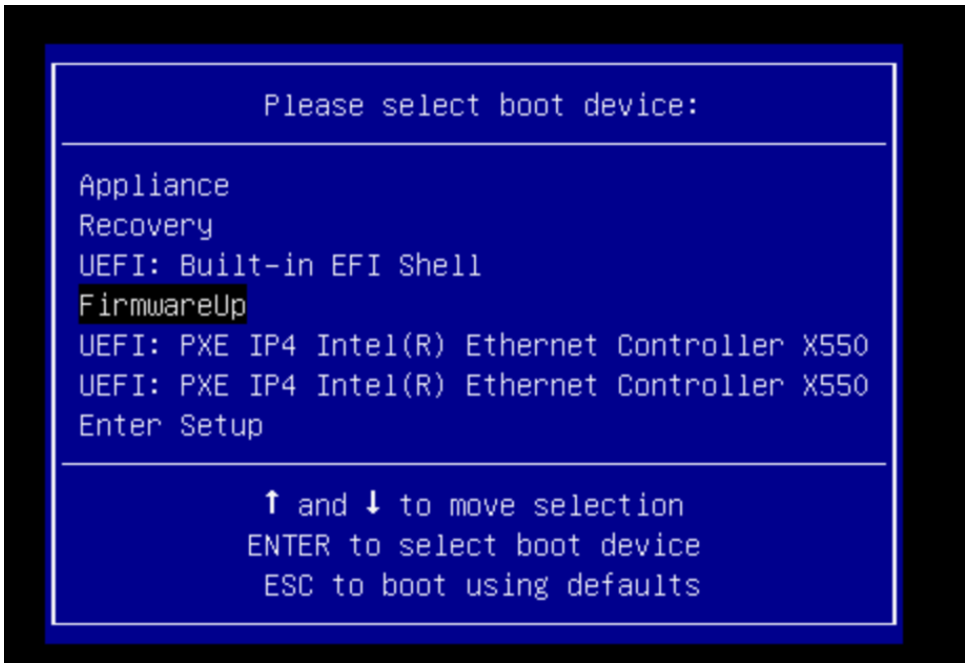
ステップ 1 Cisco Secure Malware Analytics アプライアンスの電源を投入またはリブートします。リブートするには、**[操作（Operations）**] タブをクリックし、**[電源（Power）]**を選択して、**[リブート（Reboot）]** ボタンをクリックします。アプライアンスが再起動し、[BIOS] ウィンドウが開きます。

ステップ 2 ブート プロセス中に**F6 を繰り返し押して** 、UEFI（Unified Extensible Firmware Interface）ブート メニューを表示します。

ステップ 3 矢印キーを使用して **[FirmwareUp]** オプションに移動し、 **Enter キー**を押します。

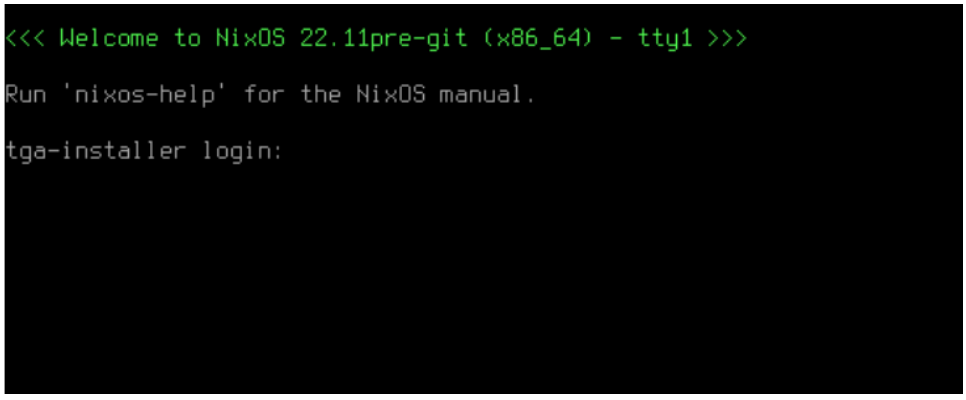
FirmwareUp によるファームウェアの更新

図 *77 : FirmwareUp*

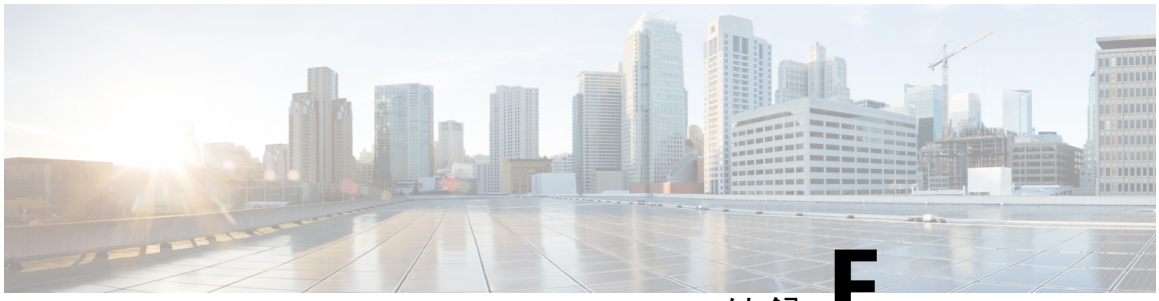


更新プロセスが自動的に開始されます。

（注）
次のログイン画面が表示された場合は、無視しても問題なく、更新プロセスが続行されます。



ファームウェアの更新が完了すると、アプライアンスがリブートします。その後、アプライアンスの通常のソフトウェアが通常どおりにロードされます。



付録 E

CIMC の設定

Cisco Integrated Management Controller（CIMC）は、サーバーを管理するために使用されるユーザー インターフェイスです。この付録には、CIMC ユーティリティを使用したリモートサーバー管理の設定に関する次の情報が含まれます。

CIMC 設定ユーティリティの使用

サーバーを起動すると、シスコの画面が表示され、Cisco Integrated Management Controller（CIMC）設定ユーティリティを開始できます。CIMC インターフェイスはリモート サーバー管理に使用できます。

このユーティリティを使用するには、モニターとキーボードを Cisco Secure Malware Analytics アプライアンスに直接接続する必要があります。

（注） CIMC は、Cisco Secure Malware Analytics M5 アプライアンスサーバーではサポートされていません。

手順

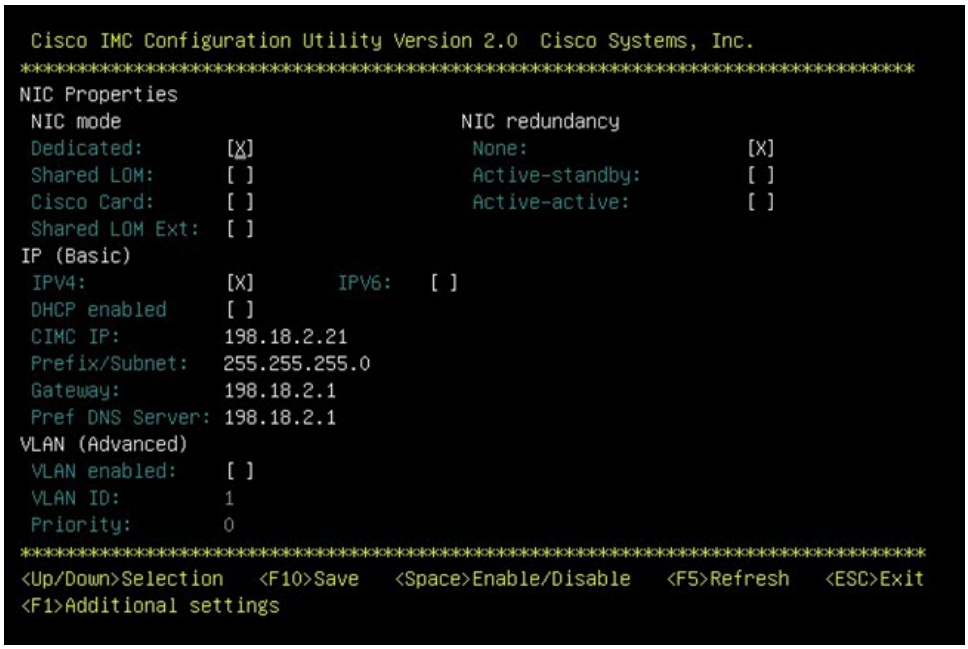
ステップ 1 サーバーの電源をオンにします。

CIMC の設定

図 *78 :* シスコの画面

ステップ 2 メモリチェックが完了したら、**F8** を押して CIMC 設定ユーティリティを開始します。

図 *79 : CIMC Configuration Utility*



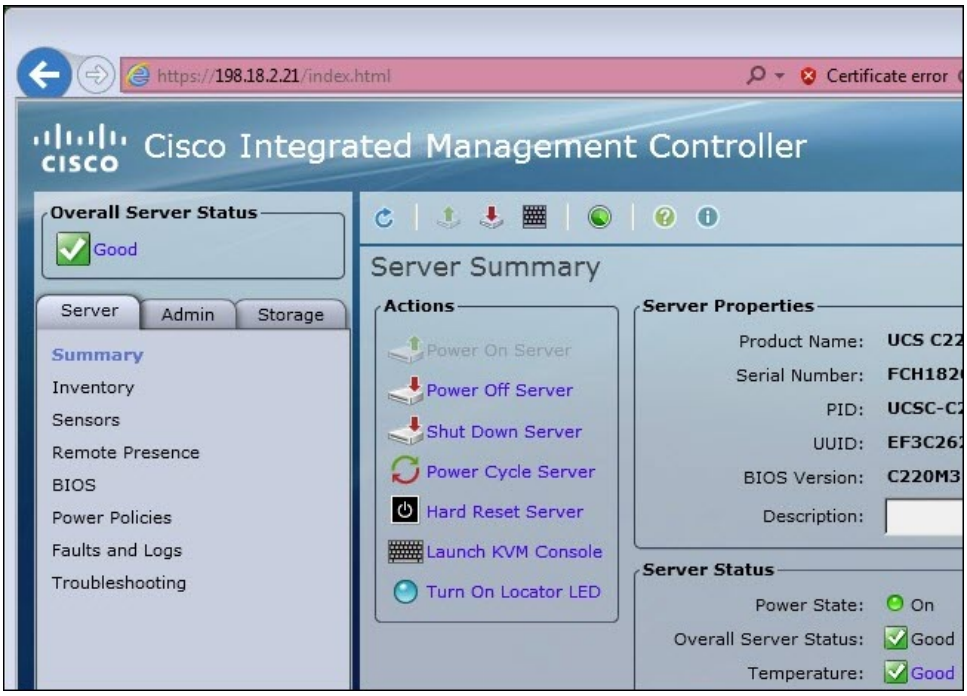
ステップ 3 CIMC 設定ユーティリティで、リモートサーバー管理に使用できる IP アドレスを設定します。

ステップ 4 設定を保存し、ユーティリティを終了します。

ステップ 5 Web ブラウザで「**https://<CIMC-IP address>/**」と入力して、CIMC インターフェイスを開きます。

ステップ 6 初期**ユーザー名**（admin）と**パスワード**（password）を入力します。

図 *80 : Cisco Integrated Management Controller*（*CIMC*）インターフェイス



CIMC インターフェイスを使用して、サーバーの正常性を表示したり、KVM を開いて残りのセットアップ手順をリモートで実行したりすることができるようになりました。

CIMC の設定

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。