Cisco Threat Grid アプライアンス バージョン 2.9 設定および構成ガイド

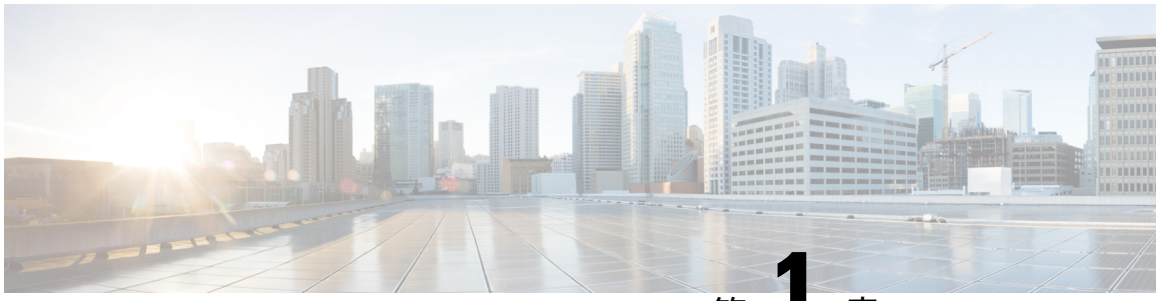
初版：2019 年 12 月 12 日

最終更新：2019 年 12 月 17 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

この章では、Cisco Threat Grid アプライアンスの概要、対象読者、および関連する製品ドキュメントへのアクセス方法について説明します。ここでは、次の項目について説明します。

Cisco Threat Grid アプライアンスについて

Cisco Threat Grid アプライアンスは、詳細な脅威分析とコンテンツによる高度なマルウェア分析を、安全で高度にセキュアなオンプレミスで提供します。Threat Grid アプライアンスは、Cisco Threat Grid M5 アプライアンスサーバ（v 2.7.2 以降）にインストールされた完全な Threat Grid マルウェア分析プラットフォームを提供します。さまざまなコンプライアンスおよびポリシーの制限に基づいて運営している組織が、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-M3（TG5000）および Cisco UCS C220 M4（TG5400）サーバは、引き続き Threat Grid アプライアンスで使用できますが、サーバのサポートは終了しています。手順については、『*Cisco Threat Grid* アプライアンス設定および構成ガイド』（バージョン 2.7 以前）のサーバの設定の章を参照してください。

銀行や医療サービスなどの機密データを扱う多くの組織は、マルウェアアーティファクトなどの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 Threat Grid 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。

Threat Grid 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つのアクティビティおよび特性の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事例に照らして、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 2.9 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 *2.9Mfg* の変更点 - *2019* 年 *12* 月 *17* 日

機能または更新	セクション
変更なし	

表 *2 :* バージョン *2.9* の変更点 - *2019* 年 *12* 月

機能または更新	セクション
管理ポートを無効にするための Threat Grid Shell コマンド。	Threat Grid シェル（tgsh）
ネットワークインターフェイスを更新して、管理ポートを無効にする機能が管理インターフェイスに含まれるようにしました。	ネットワーク インターフェイス
Threat Grid Web ポータル UI 管理者パスワードを更新	ログイン名とパスワード（デフォルト） アプライアンス設定のテスト
サポート情報が更新されました。	Threat Grid のサポート

対象読者

新しいアプライアンスをマルウェアの分析に使用する前に、組織のネットワークに合わせてセットアップおよび構成する必要があります。このガイドは、新しい Threat Grid アプライアンスの設定および構成タスクを担当するセキュリティチームの IT スタッフを対象としています。

このドキュメントでは、新しい Threat Grid アプライアンスで分析用のマルウェア サンプルを送信できるようにするまでの初期セットアップと設定の方法について説明します。

製品に関する資料

Cisco Threat Grid 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。

- *Cisco Threat Grid アプライアンス リリースノート*
- *Cisco Threat Grid バージョン ルックアップ テーブル*
- *Cisco Threat Grid アプライアンス管理者ガイド*
- *Cisco Threat Grid M5 ハードウェア設置ガイド*

（注） Cisco Threat Grid M5 アプライアンスは、Threat Grid バージョン 3.5.27 以降、および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。

（注） 以前のバージョンの Cisco Threat Grid アプライアンス製品マニュアルは、Threat grid インストールとアップグレードにあります。

Threat Grid Portal UI オンラインヘルプ

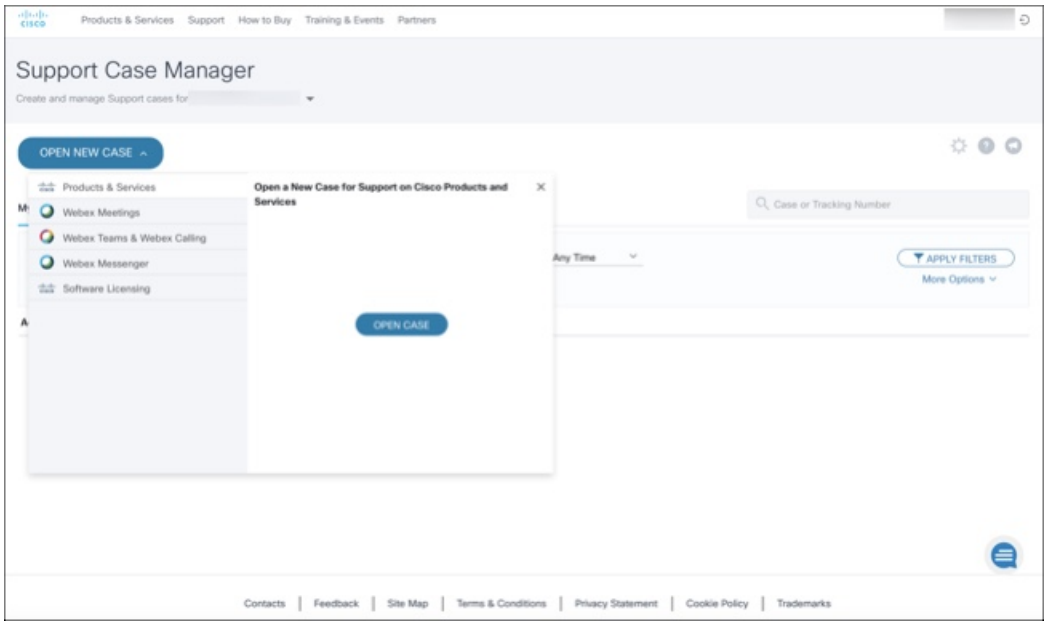
リリースノート、Threat Grid オンラインヘルプ、API ドキュメント、およびその他の情報を含む Threat Grid Portal ユーザドキュメントは、ユーザインターフェイス上部のナビゲーションバーにある [Help] メニューから入手できます。

Threat Grid のサポート

Threat Grid に関するご質問や支援が必要な場合は、https://mycase.cloudapps.cisco.com/case でサポートケースをオープンしてください。

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

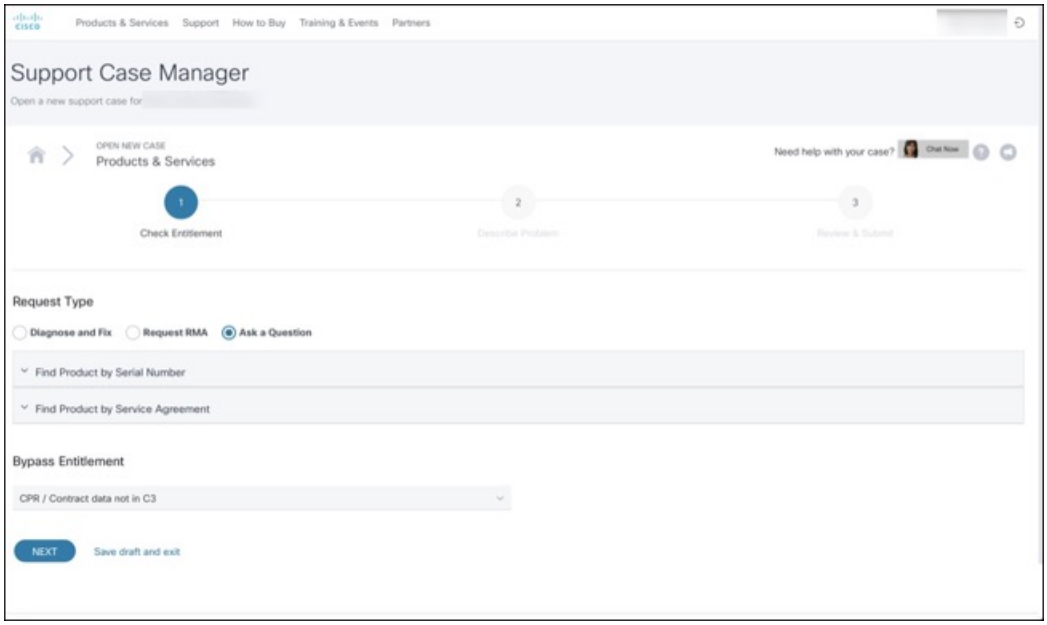
図 *1*: 新しいケースをオープンする



ステップ 2 [Ask a Question] オプションボタンをクリックし、使用している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。これは、Threat Grid 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。

ステップ 3 エンタイトルメントをバイパスする場合は、[Contract Data not in C3] を選択し、[Next] をクリックします。

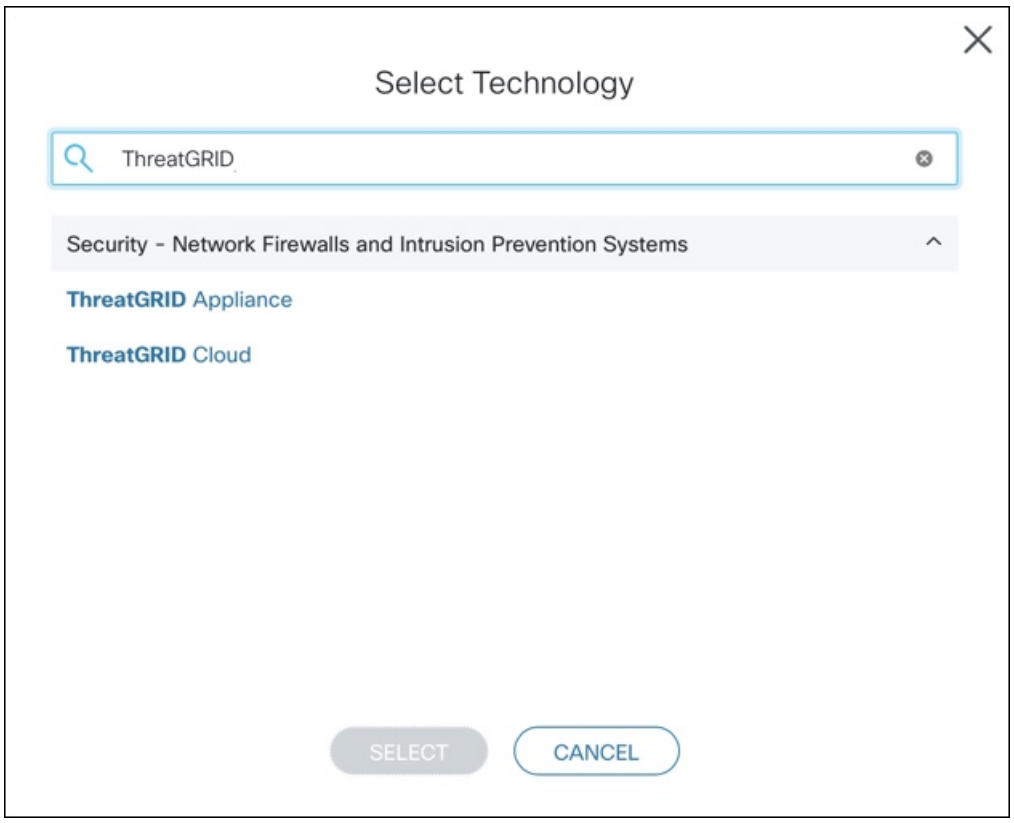
図 *2*: エンタイトルメントのチェック



ステップ 4 [Describe Problem] ページで、問題のタイトルと説明をそれぞれ [Title] と [Description] に入力します（タイトルには Threat Grid を含めます）。

ステップ 5 [Manually select a Technology] をクリックして、**ThreatGRID** を検索します。

図 *3*:テクノロジーの選択



ステップ 6 リストから **ThreatGRID Appliance** を選択し、[Select] をクリックします。

ステップ 7 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オープンできない場合は、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
- **ワールドワイド連絡先**：https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

サポートを要求する方法の詳細については、以下を参照してください。

- 次のブログ投稿を参照してください：**Changes to the Cisco Threat Grid Support Experience**（https://community.cisco.com/t5/security-blogs/changes-to-the-cisco-threat-grid-support-experience/ba-p/3911407）
- 次の**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：https://www.cisco.com/c/en/us/support/index.html

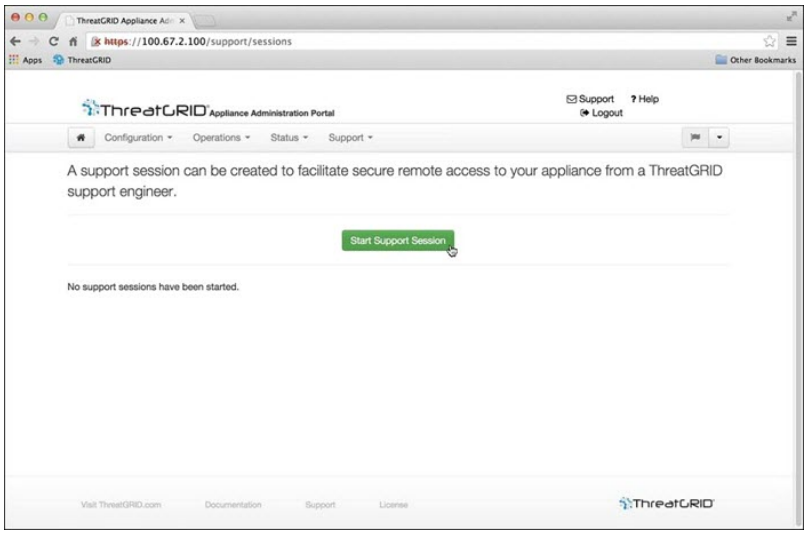
サポート モードの有効化

Threat Grid 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、Threat Grid 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には影響しません。

OpAdmin Portal の [Support] メニューからサポートモードを有効にすることができます。サポートモードは、TGSH ダイアログから、従来の Face Portal UI から、またリカバリモードでの起動時に有効にすることもできます。

ステップ 1 OpAdmin Portal で [Support] メニューをクリックし、[Live support Session] を選択します。

図 *4 : OpAdmin* のライブサポートセッションの開始



ステップ 2 [Start Support Session] をクリックします。

（注） OpAdmin 設定ウィザードを終了して、ライセンスを適用する前にサポートモードを有効にすることができます。

サポート スナップショット

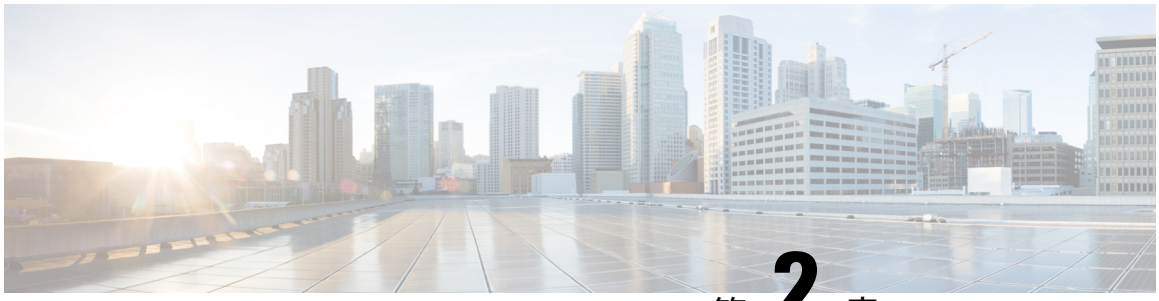
基本的にサポートスナップショットは実行中のシステムのスナップショットであり、ログ、psoutput などが含まれ、サポートスタッフによる問題のトラブルシューティングに役立ちます。

ステップ 1 SSH がサポート スナップショット サービスに指定されていることを確認します。

ステップ 2 [Support] メニューから、[Support Snapshots] を選択します。

ステップ 3 スナップショットを取得します。

ステップ 4 スナップショットを取得したら、**.tar** または **.gz** としてダウンロードすることができます。または、[Submit] を押して、Threat Grid スナップショット サーバにスナップショットを自動的にアップロードできます。



第 2 章

計画

Cisco Threat Grid 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 Threat Grid ソフトウェアを備える Linux サーバです。新しい Threat Grid アプライアンスを受け取ったら、オンプレミスのネットワーク環境に応じて設定および構成を行う必要があります。

この章には、構成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要件に関する次の情報が含まれています。

対応ブラウザ

Threat Grid 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はサポートされません。

環境要件

Threat Grid アプライアンス（v2.7.2 以降）は、Threat Grid M5 アプライアンスサーバ上で展開されます。Threat Grid 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。Threat Grid アプライアンスをクラスタリングしている場合は、各アプライアンスの Clust インターフェイスに追加の SFP+ モジュールが必要となります。

（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 Threat Grid 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 *5 : Cisco 1000BASE-T* 銅線 *SFP*（*GLC-T*）

サーバにモニタを接続できます。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 サーバ上で）。

（注） CIMC は、Threat Grid 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

Threat Grid 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。

- **管理**：Threat Grid 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。
  - OpAdmin 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、Threat Grid 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 OpAdmin Portal 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
  - Threat Grid 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
  - AMP for Endpoints 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
- **ダーティ**：ダーティネットワークは、Threat Grid 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 Threat Grid ソフトウェアからの通知に使用されるメールサーバの解決以外の目的に使用される DNS サーバは、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 AMP for Endpoints プライベート クラウドの統合に使用されます。AMP for 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 サーバを OpAdmin インターフェイスに構成できます。

詳細については、『Cisco Threat Grid アプライアンス管理者ガイド』を参照してください。

NTP サーバ アクセス

NTP サーバはダーティ ネットワークからアクセスできる必要があります。

統合

Threat Grid アプライアンスを他のシスコ製品（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、AMP for 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、『*Cisco Threat Grid*アプライアンス管理者ガイド』を参照してください。

DHCP

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、『*Cisco Threat Grid* アプライアンス管理者ガイド』の「DHCPの使用」の項に記載されている手順に従ってください。

ライセンス

Cisco Threat Grid からライセンスとパスワードを受信します。

ライセンスに関して不明な点がある場合は、Threat Grid のサポートにお問い合わせください。

レート制限

API レート制限は、ライセンス契約の条件に基づいて Threat Grid 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。詳細な説明については、Threat Grid Portal UI オンラインヘルプのよくある質問を参照してください。

組織とユーザ

Threat Grid 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、Threat Grid の初期組織を作成してユーザ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。この作業では、要件に応じて、複数の組織やユーザ間での計画と調整が必要になる場合があります。

『*Cisco Threat Grid アプライアンス管理者ガイド*』の「新しい組織の作成」の項を参照してください。ユーザの管理の詳細については、Threat Grid Portal のヘルプを参照してください。

変更点（Updates）

Threat Grid アプライアンスの更新をインストールする場合は、事前に初期のアプライアンス設定および構成手順が**完了している**必要があります。初期設定の完了直後に、更新を確認することをお勧めします（「Threat Grid アプライアンスの更新のインストール」を参照）。

Threat Grid 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るまでダウンロードできません。また、更新プロセスでは、アプライアンスの初期設定が完了している必要があります。更新は順に行う必要があります。

（注） 更新用に SSH が指定されていることを確認してください。

ユーザ インターフェイス

サーバがネットワークに正常に接続され、電源が入ると、複数のユーザインターフェイスを使用して Threat Grid アプライアンスを設定できるようになります。

（注） LDAP 認証は、TGSH ダイアログおよび OpAdmin（v2.1.6 以降）で利用できます。

TGSH ダイアログ

TGSH ダイアログインターフェイスは、ネットワーク インターフェイスの設定に使用します。TGSH ダイアログは、Threat Grid アプライアンスが正常に起動すると表示されます。

TGSH ダイアログへの再接続

TGSH ダイアログはコンソールで開いたままになっており、アプライアンスにモニタを接続するか、CIMC が設定されている場合はリモート KVM 経由でアクセスできます。

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

TGSH ダイアログに再接続するには、ユーザ **threatgrid** を使用して管理 IP アドレスに SSH 接続します。

必要なパスワードは、TGSH 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 OpAdmin Portal の設定 設定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。

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、TGSH ダイアログで [CONSOLE] を選択します。

（注） OpAdmin は Threat Grid ユーザ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すべて OpAdmin 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、Threat Grid 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 OpAdmin または TGSH ダイアログを使用する必要があります。

OpAdmin Portal

これは主要な Threat Grid GUI 設定ツールです。ライセンス、電子メールホスト、SSL 証明書など、Threat Grid アプライアンス設定の多くは OpAdmin からのみ実行できます。

Threat Grid Portal

この Threat Grid ユーザ インターフェイス アプリケーションはクラウド サービスとして使用可能で、Threat Grid アプライアンスにもインストールされます。Threat Grid Cloud サービスと、Threat Grid アプライアンスに含まれる Threat Grid Portal との間で通信は行われません。

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**。 • OpAdmin UI トラフィック • TGSH ダイアログ用の SSH（受信） • 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。 • 管理ポートは（tgsh シェルから）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 Threat Grid アプライアンスは、クリーンポートとダーティ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 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、Threat Grid アプライアンスは機能しなくなります（または、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 サーバへの発信接続） • SSH（TGSH ダイアログの受信） • syslog（設定済み syslog サーバへの発信） • ESA/WSA と CSA の統合 • AMP for Endpoints プライベート クラウドの統合 • DNS（オプション） • LDAP（発信）

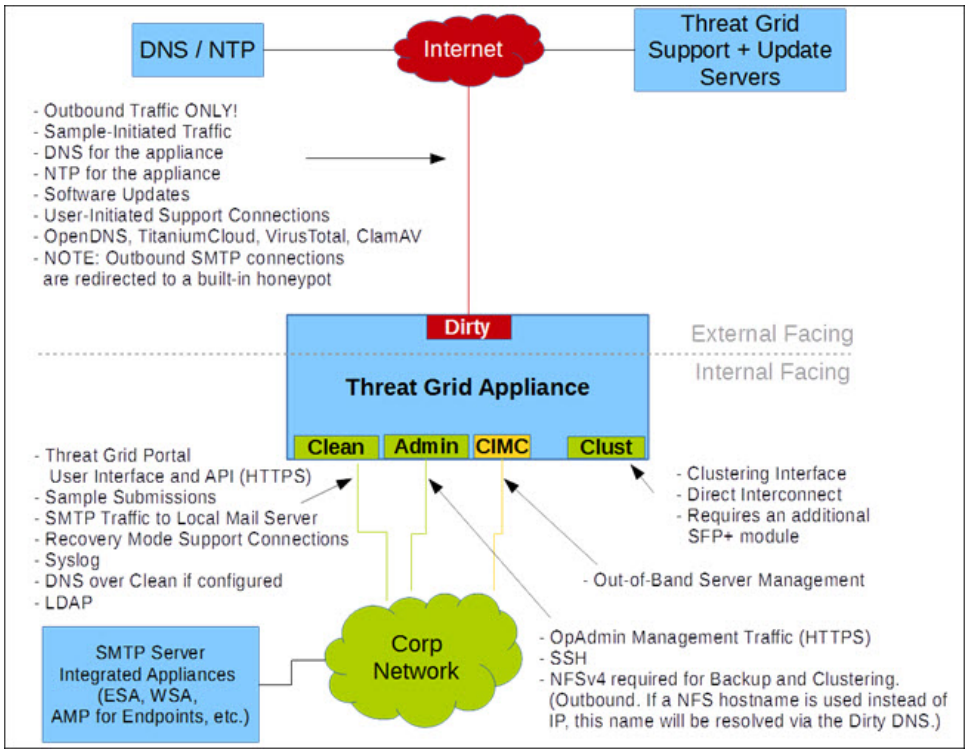
インターフェイス	説明
ダーティ	ダーティネットワークに接続します。インターネットアクセスが必要です。発信のみ。 プライベート IP に送信されるトラフィックは、ネットワーク出口のローカリゼーション ファイアウォールでドロップされるため、ダーティインターフェイスには独自の DNS（プライベート IP）を使用しないようにしてください。 • DNS （注） AMP for Endpoints プライベートクラウドとの統合を設定し、AMP for Endpoints アプライアンスのホスト名がダーティインターフェイスで解決できない場合、クリーンインターフェイスを使用する別の DNS サーバを OpAdmin に設定できます。 • NTP • Updates • 通常の動作モードでの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 • リカバリ モード サポート セッション（発信） • OpenDNS、TitaniumCloud、VirusTotal、ClamAV • 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	推奨。Cisco Integrated Management Controller（CIMC）インターフェイスが設定されている場合は、サーバの管理とメンテナンスに使用できます。詳細については、『*Cisco Threat Gridアプライアンス管理者ガイド*』を参照してください。 （注） CIMC は、Threat Grid 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、Threat Grid 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 *6:* ネットワーク インターフェイスの設定図



（注） Threat Grid 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 の管理インターフェイスへのアクセスを有効にします。

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	宛先	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）	サンプルからの発信トラフィックを許可します。（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	宛先	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	宛先	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	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	宛先	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	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

送信元	宛先	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	AMP プライベート クラウド	TCP	443	許可（Allow）	任意。AMP for Endpoints 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	UDP	514	許可（Allow）	syslog メッセージと Threat Grid 通知を受信するように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	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	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 インターフェイスによる着信

送信元	宛先	プロトコル	ポート	操作	コメント
ユーザ サブネット	クリーン インターフェイス	TCP	22	許可（Allow）	TGSH ダイアログへの SSH 接続を許可します。
ユーザ サブネット	クリーン インターフェイス	TCP	80	許可（Allow）	アプライアンスの API と Threat Grid ユーザ 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 サブネット	クリーン インターフェイス	TCP	443	許可（Allow）	アプライアンスの API と Threat Grid ユーザ インターフェイス。
ユーザ サブネット	クリーン インターフェイス	TCP	9443	許可	Threat Grid UI Glovebox 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	宛先	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	TCP	2049	許可（Allow）	任意。Threat Grid 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	宛先	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）	TGSH ダイアログへの 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）	OpAdmin Portal インターフェイス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）	OpAdmin Portal インターフェイス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

送信元	宛先	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）	Threat Grid サポートへの接続を許可します。
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。

送信元	宛先	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	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。

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（User）	ログイン/パスワード
OpAdmin およびシェルユーザ	最初の Threat Grid/TGSH ダイアログでランダムに生成されたパスワードを使用し、次に OpAdmin 設定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、『*Cisco Threat Grid アプライアンス管理者ガイド*』の「管理者パスワードのリセット」の項を参照してください。
Threat Grid Web Portal UI 管理者	Login: **admin** Password：最初の OpAdmin パスワードを使用して初期化します。その後、パスワードは固有になります。
CIMC	Login: **admin** Password: **password**

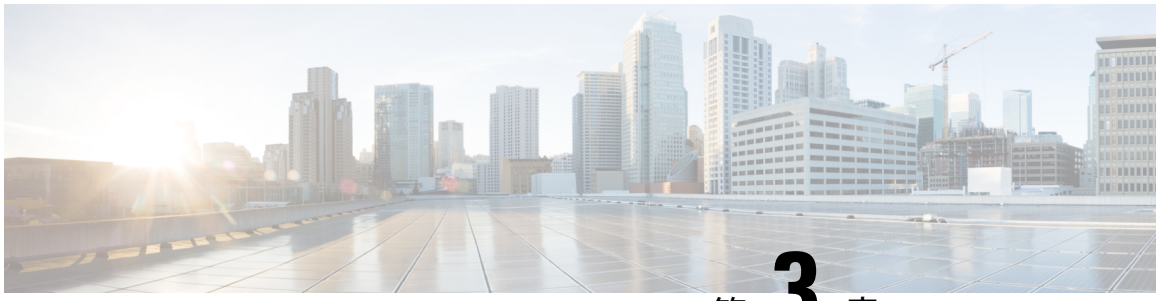
設定と構成の概要

このドキュメントでは、次の設定および初期構成の手順を説明します。

- 初期ネットワーク設定
- OpAdmin Portal の設定
- 更新のインストール
- アプライアンス設定のテスト

『*Threat Grid* アプライアンス管理者ガイド』に記載されているとおり、OpAdmin Portal で、残りの管理構成タスク（ライセンスのインストール、電子メールサーバ、SSL 証明書など）を完了します。

初期設定手順を完了するには約 1 時間かかります。



第 3 章

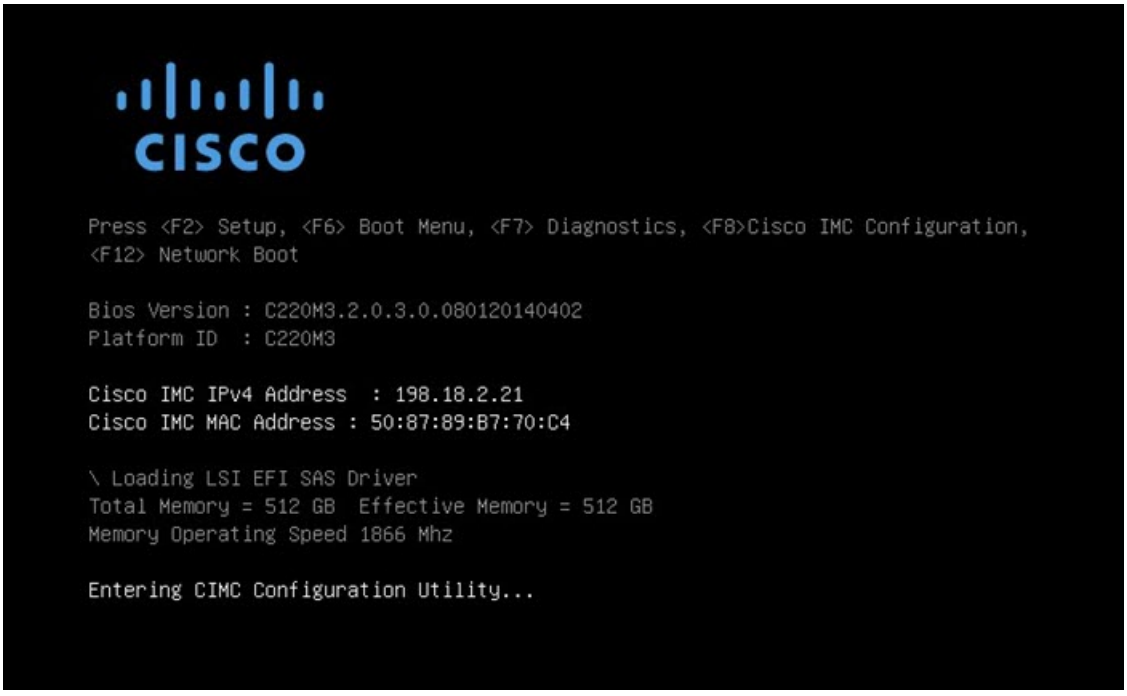
初期ネットワーク設定

この章では、TGSH ダイアログを使用してネットワークの初期設定を完了する手順について説明します。内容は次のとおりです。

アプライアンスの電源オンと起動

サーバ周辺機器、ネットワーク インターフェイス、電源ケーブルを接続したら、Threat Grid M5 アプライアンスの電源を入れ、起動するまで待機します。シスコの画面が短時間表示されます。

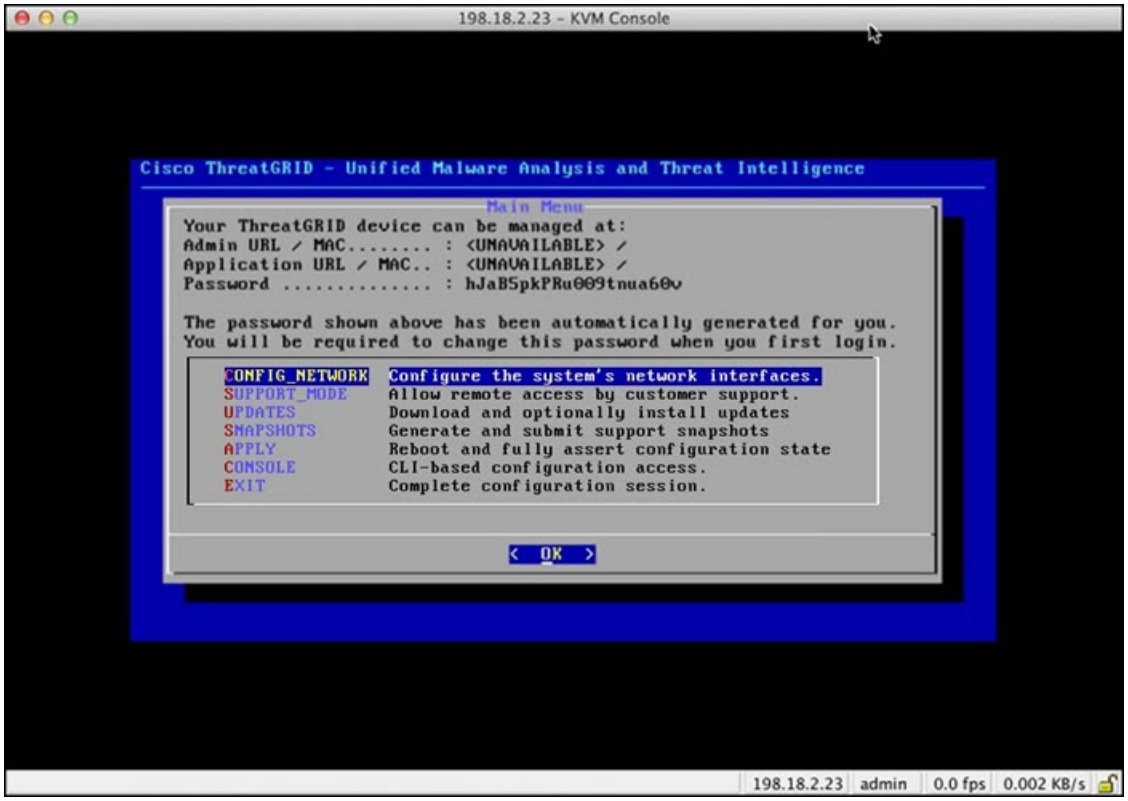
図 7: ブートアップ時のシスコ画面



（注） このインターフェイスを設定する場合は、メモリチェックが完了した後に **F8** を押します。『*Cisco Threat Grid アプライアンス管理者ガイド*』の付録「CIMC の設定」を参照してください。

サーバ起動と接続が正常終了すると、コンソールに TGSH ダイアログが表示されます。

図 *8 : TGSH* ダイアログ



ネットワーク インターフェイスの接続がまだ設定されていないため OpAdmin Portal に到達できず、このタスクを実行できないため、[Admin URL] は利用不可として示されています。

重要 **TGSH ダイアログ**には、初期管理者パスワードが表示されます。このパスワードは、この後の構成手順でOpAdmin Portalインターフェイスにアクセスし、インターフェイスを構成するために必要となります。パスワードを別のテキストファイルでメモ（コピーアンドペースト）しておきます。

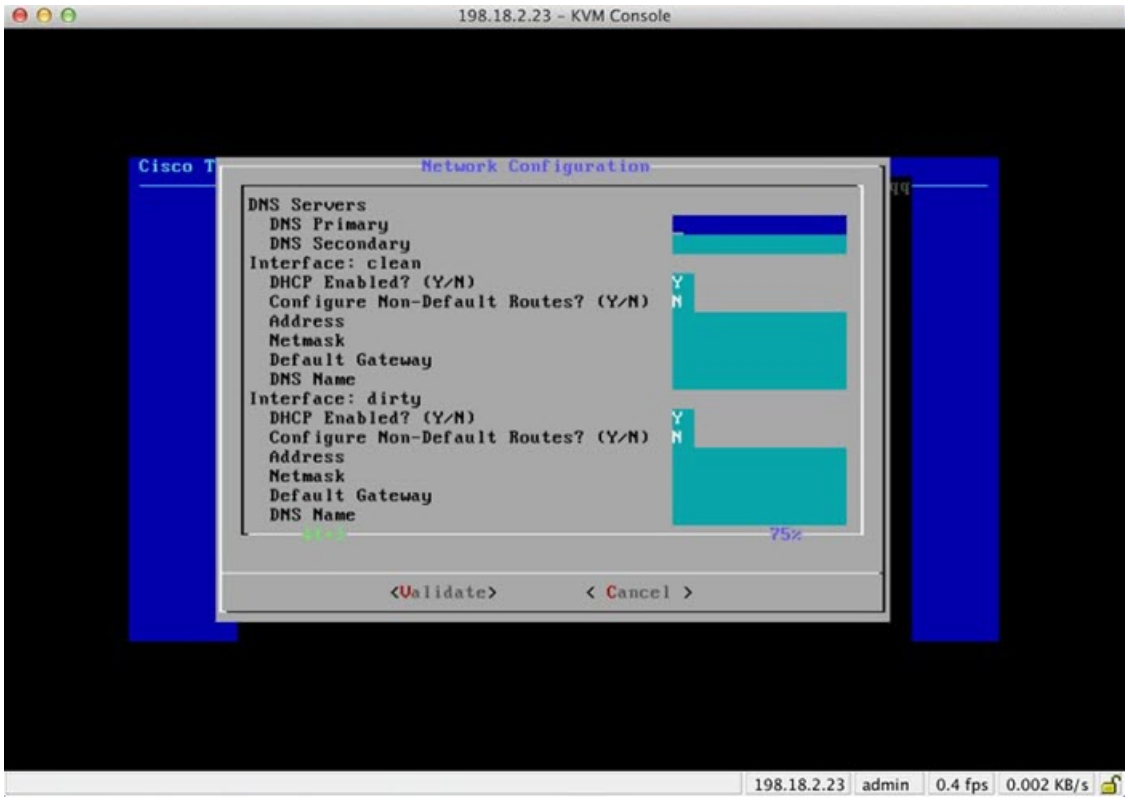
TGSH ダイアログを使用したネットワークの設定

初期ネットワーク設定は、TGSH ダイアログで行います。基本設定が完了すると、OpAdmin ポータルへのアクセスが許可されます。このポータルではその他の設定タスクを実行できます。

（注） DHCPユーザの場合、次の手順では、静的IPアドレスを使用していることを想定しています。DHCP を使用して IP を取得している場合は、『*Threat Grid Appliance* 管理者ガイド』を参照してください。

ステップ 1 TGSH ダイアログで、[CONFIG_NETWORK] を選択します。[Network Configuration] コンソールが開きます。

図 *9 : TGSH* ダイアログ：*[Network Configuration]* コンソール



ステップ 2 クリーン、ダーティ、および管理の各インターフェイスに対して、ネットワーク管理者から提供される設定に従い、空白のフィールドに入力します。

ステップ 3 [DHCP Enabled] を [N] に変更します。

（注） 新しい文字を入力する前に、バックスペースを押して古い文字を削除する必要があります。

ステップ 4 [Configure Non-Default Routes] フィールドを、デフォルトの [N] のままにします（追加のルートが必要ない場合）。

ステップ 5 ネットワークでクリーンネットワークに DNS 名を使用している場合は、[DNS Name] フィールドに DNS 名を入力します。

ステップ 6 ダーティ ネットワークの [DNS Name] は空白のままにします。

図 *10* : 進行中のネットワーク設定（クリーンおよびダーティ）

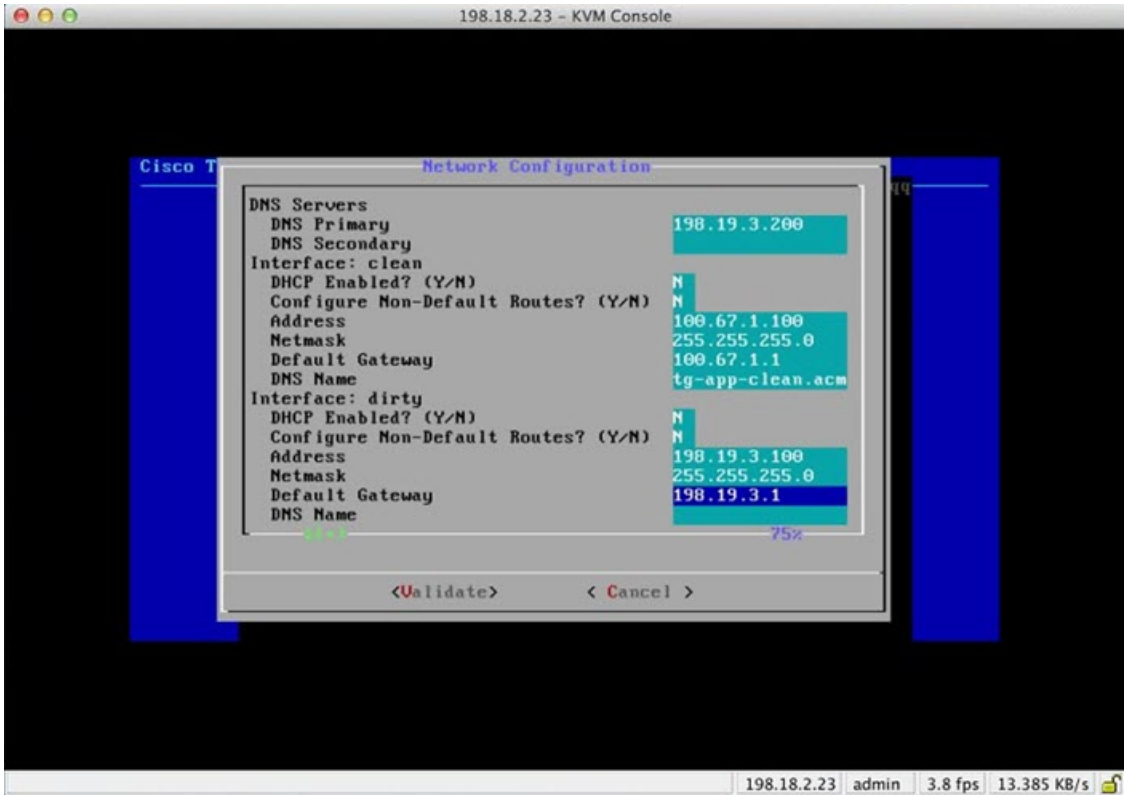


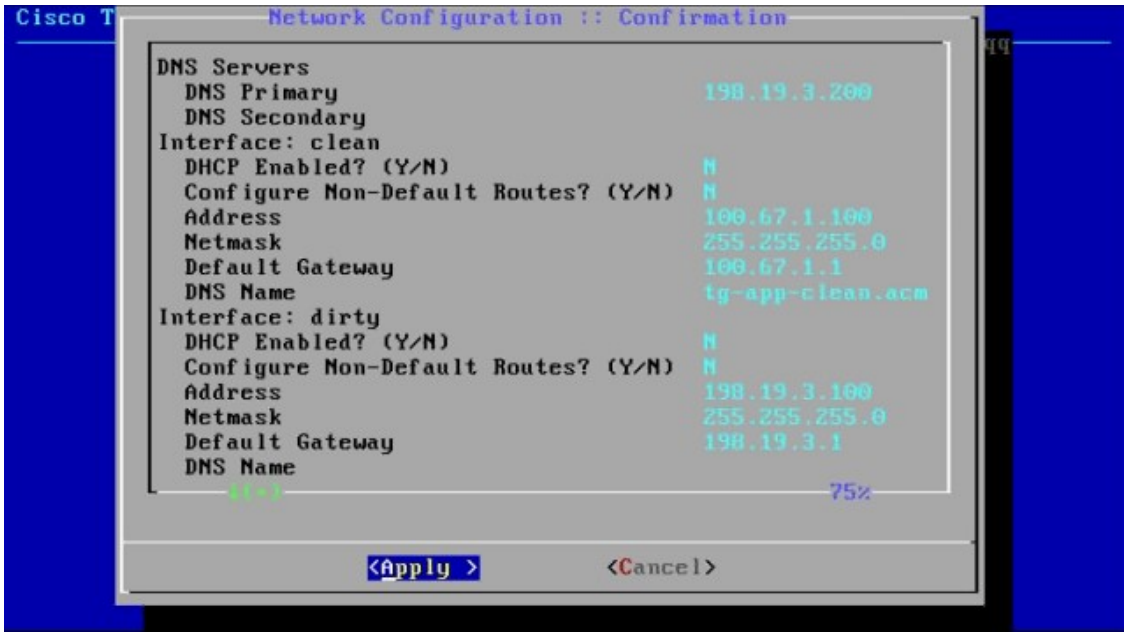
図 *11* : 進行中のネットワーク設定（管理）

ステップ 7 すべてのネットワーク設定を入力したら、Tab キーで下に移動し、[Validate] を選択して入力内容を検証します。

エラーが発生した場合は、無効な値を修正し、もう一度 [Validate] を選択します。

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

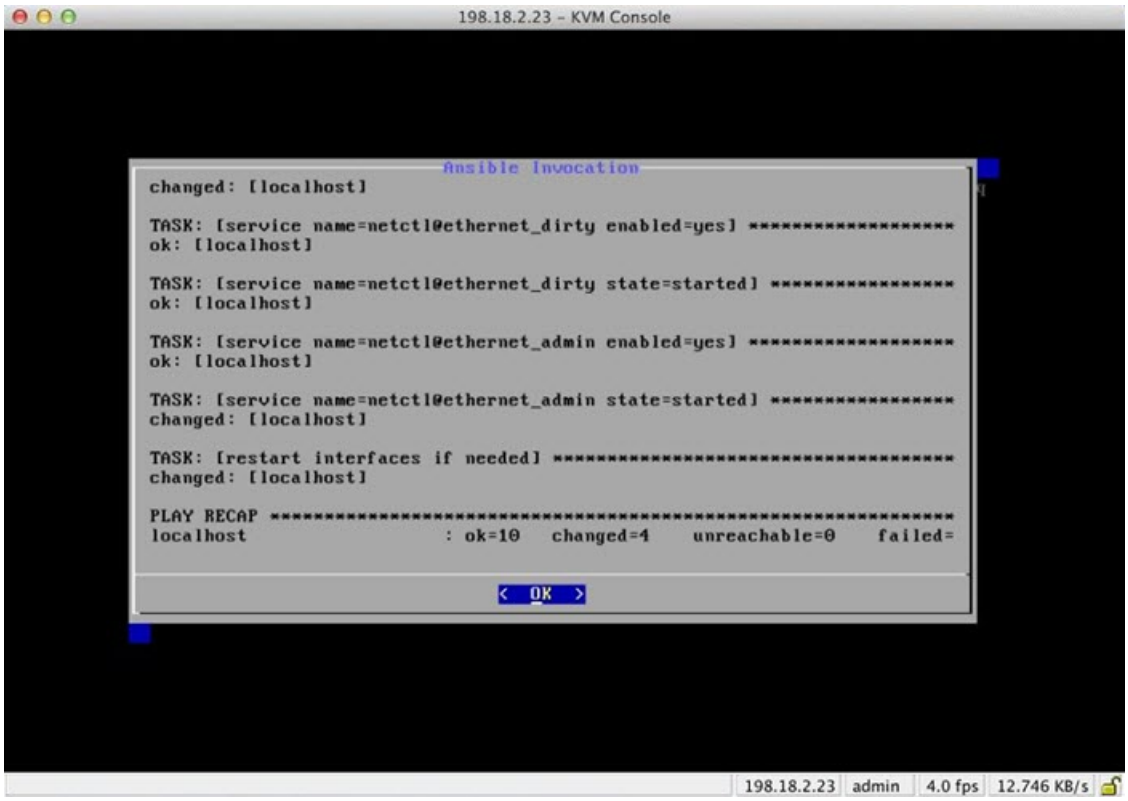
図 *12 :* ネットワーク構成の確認



ステップ 8 [Apply] を選択して各種設定を適用します。

設定が適用された後（完了までに 10 分以上かかる場合があります）、変更の詳細が表示されます。

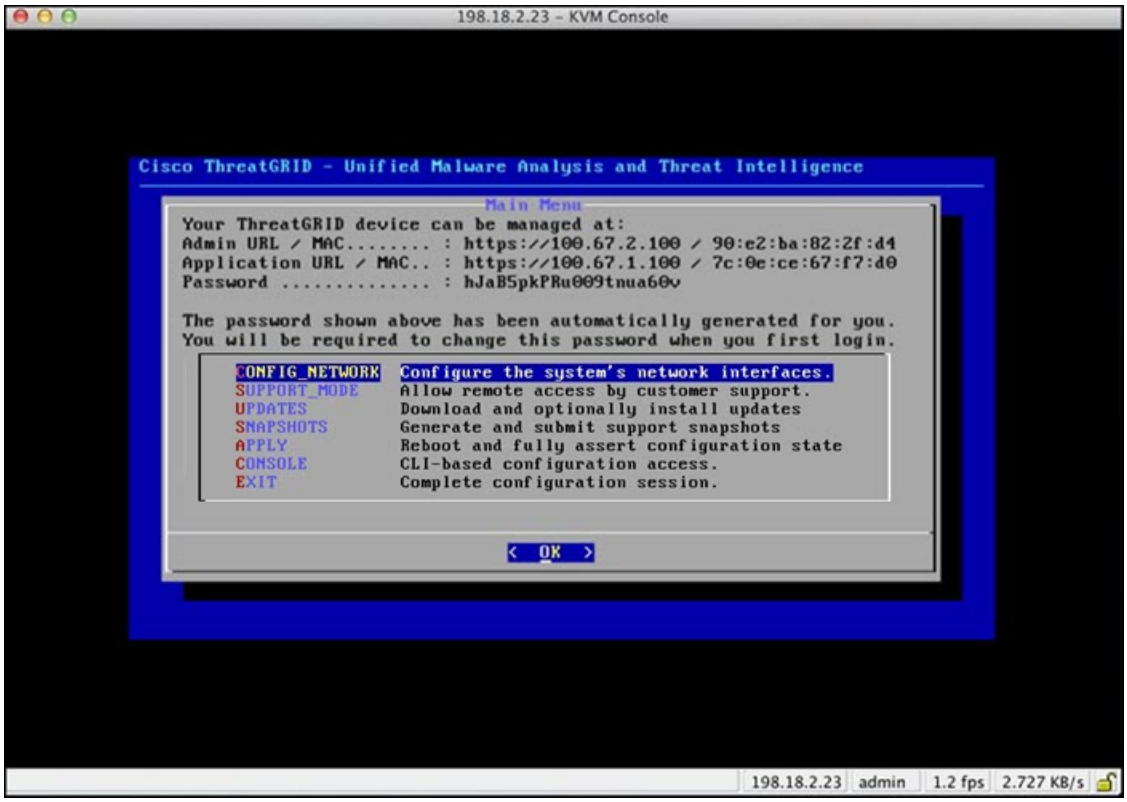
図 *13 :* ネットワーク設定：実行した変更のリスト



ステップ 9 [OK] を選択します。

[Network Configuration] コンソールが更新され、入力した IP アドレスが表示されます。

図 *14 : IP Addresses*

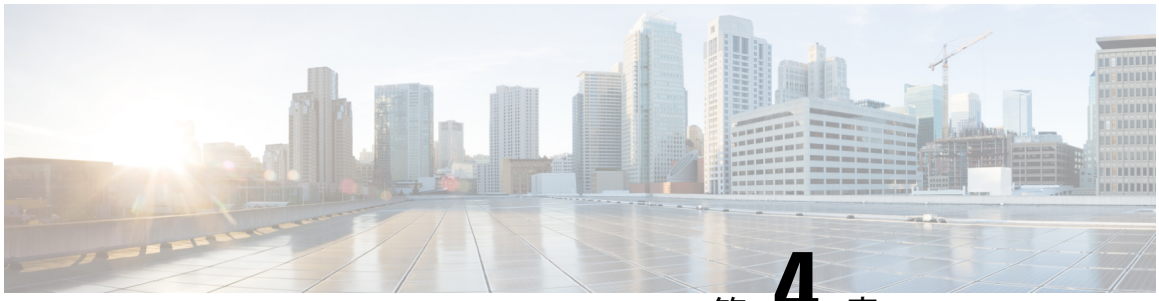


Threat Grid アプライアンスのネットワーク設定が完了しました。

（注） クリーンインターフェイスの URL は OpAdmin Portal の設定が完了するまで機能しません。

次のタスク

Threat Grid アプライアンス設定の次の手順では、「OpAdmin Portal の設定」で説明されているように、OpAdmin Portal を使用して残りの設定タスクを完了します。



第 4 章

OpAdmin Portal の設定

この章では、OpAdmin Portal を使用してアプライアンスを設定する手順について説明します。説明する項目は次のとおりです。

はじめに

OpAdmin Portal は、アプライアンス上の Threat Grid 管理者のポータルであり、アプライアンスの設定に推奨されるツールです。管理インターフェイスで IP アドレスを設定した後で使用できる Web ユーザ インターフェイスです。

この設定には、次の手順が含まれます。

- OpAdmin 管理者パスワードの変更
- エンドユーザライセンス契約書の確認
- ネットワーク構成設定（ウィザードを使用して設定されていないもの）の確認
- ライセンスのインストール
- NFS の設定
- 電子メールホストの設定
- 通知の設定
- 日付と時刻の設定（NTP サーバ）
- Syslog の設定
- 設定の確認とインストール

（注） 一部の設定手順では、設定ウィザードを使用しません。SSL 証明書やクラスタリングなど、ウィザードに含まれていない構成設定については、『*Cisco Threat Grid* アプライアンス管理者ガイド』を参照してください。

重要 以降のセクションの手順は、設定時の IP アドレスに割り込みが入る可能性を減らすために、1 回のセッションで完了する必要があります。

OpAdmin ポータルにログインする

Threat Grid OpAdmin ポータルにログインするには、次の手順を実行します。

ステップ 1 ブラウザで、OpAdmin portal の URL（**https://<adminIP>/** または **https://<adminHostname>/**）を入力して、Threat Grid OpAdmin のログイン画面を 開きます。

（注） ホスト名はアプライアンスのシリアル番号です（v2.7 以降）。

図 *15 : OpAdmin* のログイン画面

ステップ 2 TGSH ダイアログからコピーした初期設定の**管理者パスワード**を入力して、[Login] をクリックします。

次のタスク

[Change Admin Password]管理者パスワードの変更 （35 ページ）に進みます。

管理者パスワードの変更

初期設定の管理者パスワードは、出荷前の Threat Grid のインストール中にランダムに生成され、TGSH ダイアログにプレーンテキストとして表示されます。設定を続行する前に、初期設定の管理者パスワードを変更する必要があります。

ステップ 1 TGSH ダイアログに表示されるパスワードを、[Old Password] フィールドに入力します（このパスワードはテキストファイルに保存しているはずです）。

ステップ 2 [New Password] に新しいパスワードを入力し、[Confirm New Password][フィールドにもう一度入力します。

ステップ 3 [Change Password] をクリックします。パスワードが更新されます。

（注） 新しいパスワードは TGSH ダイアログに表示されるテキストでは表示されないため、必ずどこかに保存してください。

次のタスク

[Review End User License Agreemen]エンドユーザライセンス契約書の確認 （35 ページ）に進みます。

エンドユーザライセンス契約書の確認

ライセンス契約書を確認し、同意することを確認します。

ステップ 1 エンド ユーザ ライセンス契約書を確認します。

ステップ 2 最後までスクロールし、[I HAVE READ AND AGREE] をクリックして同意します。

（注） ライセンスをインストールする前に、設定ワークフローを実行し、ネットワークを設定することをお勧めします。

次のタスク

[Configure Network Settings]ネットワークの設定 （36 ページ）に進みます。

Configuration Wizard

設定ウィザードでは、手順を追って Threat Grid アプライアンスを設定します。

ネットワークの設定

TGSH ダイアログでスタティック ネットワーク設定を行った場合、[Network Configuration] ページに表示される IP アドレスは、Threat Grid アプライアンスのネットワーク設定時に TGSH ダイアログに入力した値を反映します。

ステップ 1 IP アドレスを確認し、正確であることを確認します。

ステップ 2 初期接続に DHCP を使用し、クリーンおよびダーティの IP ネットワークをスタティック IP アドレスに変更する必要がある場合、『Threat Grid Appliance 管理者ガイド』の「DHCP の使用」の項の手順を実行します。

次のタスク

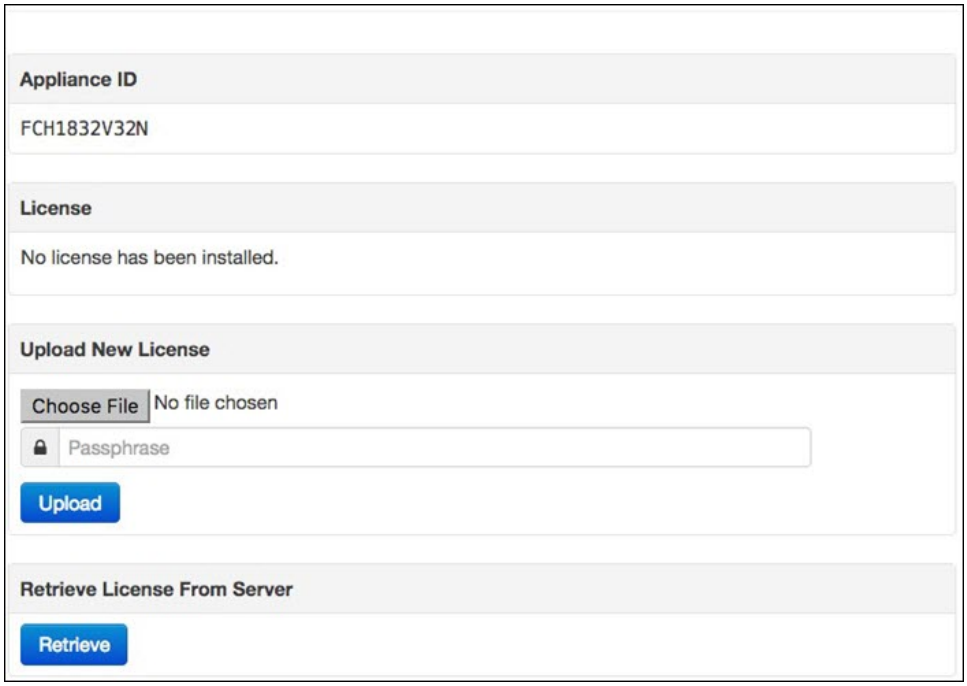
[Install License]ライセンスのインストール （36 ページ）に進みます。

ライセンスのインストール

ネットワークが設定されたら、Threat Grid ライセンスをインストールする準備が整います。

ステップ 1 ナビゲーションペインで [License] をクリックして、[License] ページを開きます。

図 *16* : インストール前のライセンスページ



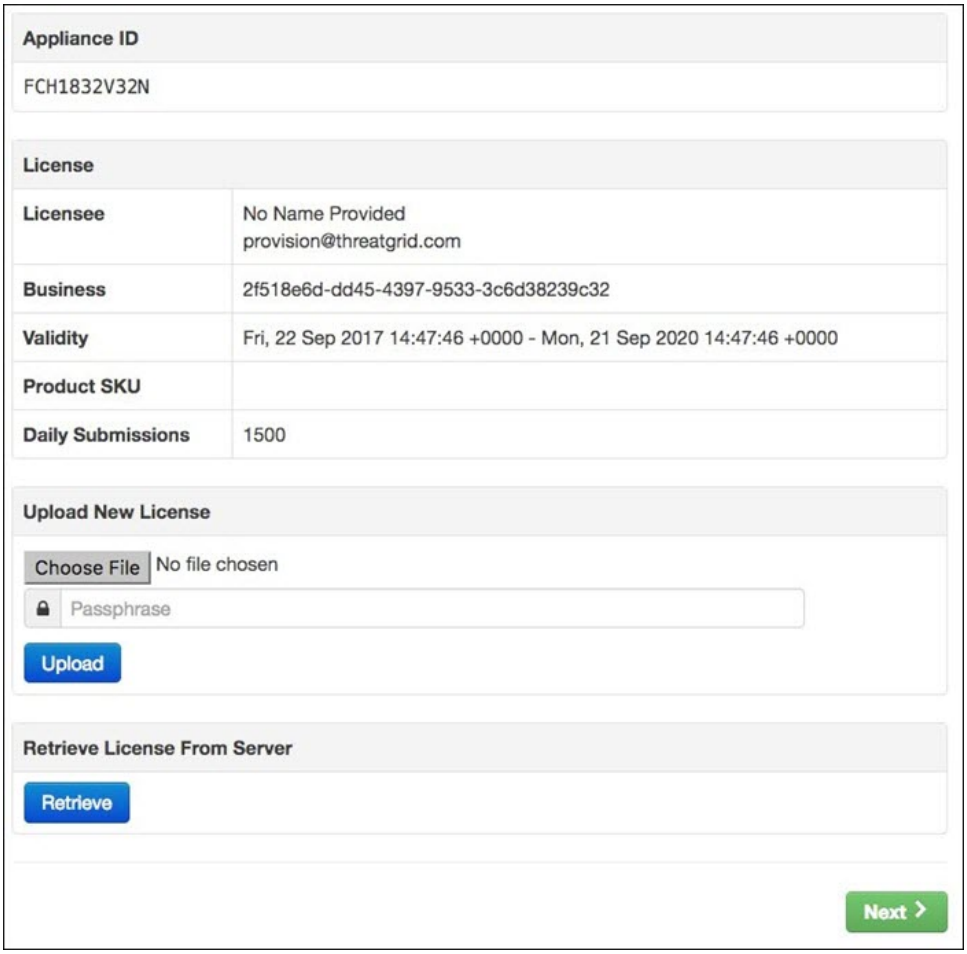
ステップ 2 [Upload New License] ペインで [Choose File] をクリックし、ファイルマネージャからライセンスを選択します。

または、サーバからライセンスを取得することもできます。アプライアンスを設置した時点ネットワークにアクセス可能な場合は、[Retrieve] をクリックするとライセンスがネットワーク経由で取得されます。

ステップ 3 [Passphrase] フィールドにライセンスのパスワードを入力します。

ステップ 4 [Upload] をクリックしてライセンスをインストールします。ページが更新され、ライセンス情報が表示されます。

図 *17:* インストールが成功した後のライセンス情報



ステップ 5 [次へ（Next）] をクリックして続行します。

次のタスク

[Configure NFS]NFS の設定 （38 ページ）に進みます。

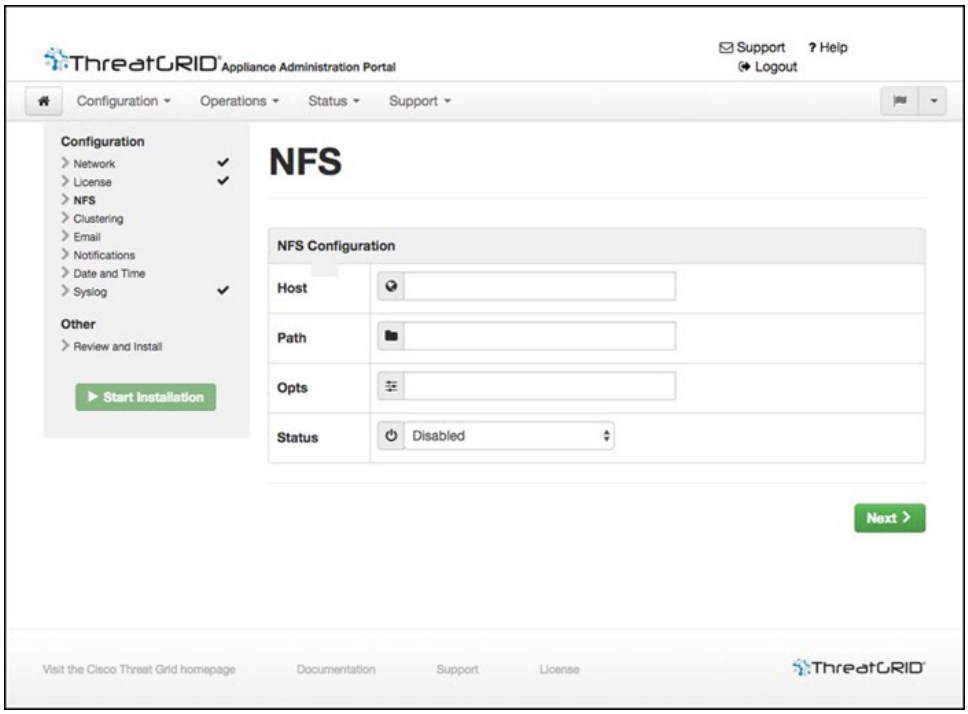
NFS の設定

ワークフローの次の手順は、NFS を設定することです。このタスクは、バックアップとクラスタリングを行うために必要です。詳細については、『*Cisco Threat Grid アプライアンス管理者ガイド*』の「NFS 要件」の項を参照してください。

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 Theat Grid 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。

ステップ 1 ナビゲーションペインで [NFS] をクリックして、[NFS] ページを開きます。

図 *18 : NFS* の設定



ステップ 2 次の情報を入力します。

- [**Host**]：NFSv4 ホストサーバ。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。
- [**Opots**]：このサーバで 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。
- [**Status**]：ドロップダウンリストから [Enabled] を選択します（キー保留中）。

ステップ 3 [次へ（Next）] 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、アップロード後に OpAdmin に表示された**キー ID** が、設定されたパスのディレクトリ名と照合されます。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 4 [次へ（Next）] をクリックして続行します。

次のタスク

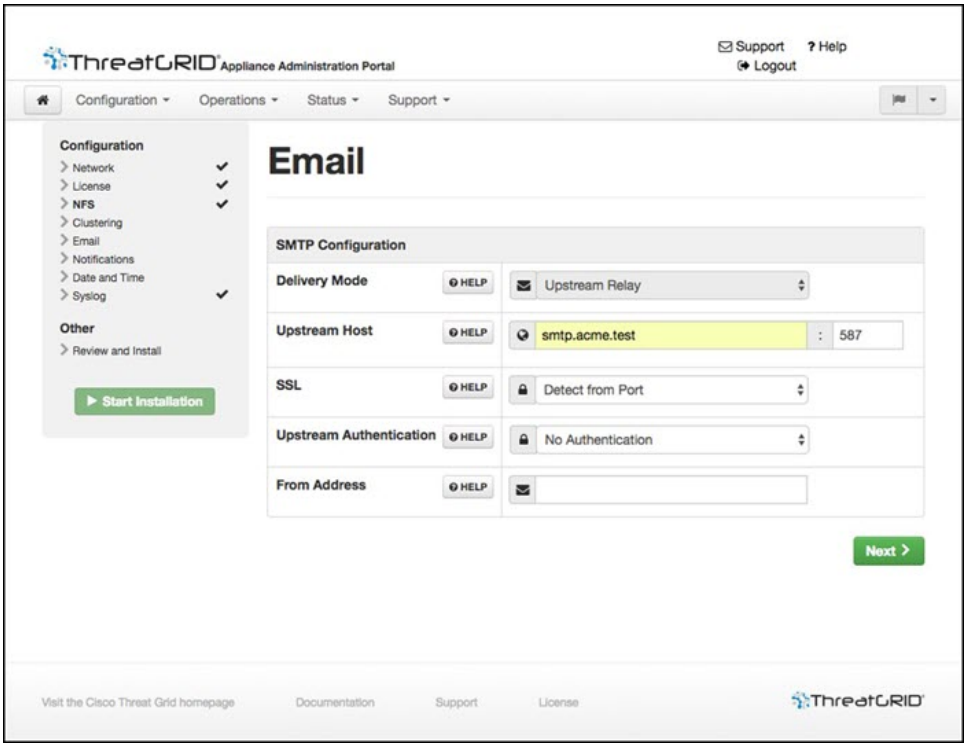
[Configure Email Host]電子メールホストの設定 （39 ページ）に進みます。

電子メールホストの設定

ワークフローの次の手順は、電子メール ホストを設定することです。

ステップ 1 ナビゲーションペインで [Email] をクリックして、[Email] ページを開きます。

図 *19* : 電子メールの設定



ステップ 2 [Upstream Host]（電子メール ホスト）の名前を入力します。
ステップ 3 ポートを **587** から **25** に変更します。
ステップ 4 その他の設定は、デフォルト値のままにします。
ステップ 5 [次へ（Next）] をクリックして続行します。

次のタスク

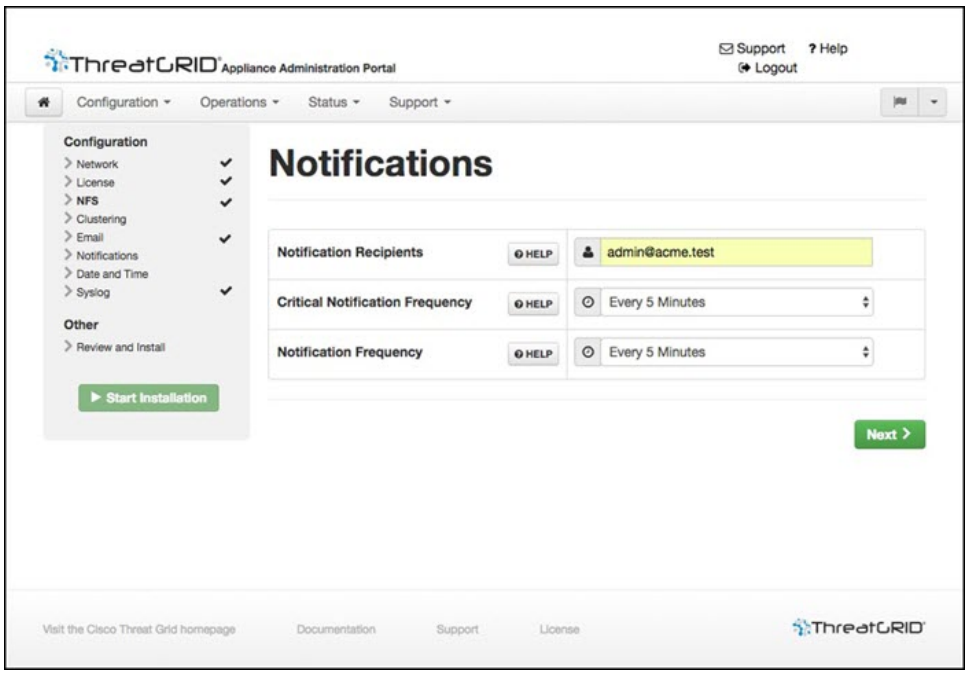
[Configure Notifications]通知の設定 （40 ページ）に進みます。

通知の設定

ワーク フローの次の手順は、1 つ以上の電子メールアドレスに定期的に配信可能な通知を設定することです。システム通知は Threat Grid インターフェイスに表示されますが、このページでは、電子メールで送信される通知も設定できます。

ステップ 1 ナビゲーションペインで [Notification] をクリックして、[Notifications] ページを開きます。

図 *20 :* 通知の設定



ステップ 2 [Notification Recipients] フィールドで、カンマで区切った 1 つ以上の電子メールアドレスを入力します。
ステップ 3 ドロップダウンリストから [Critical Notification Frequency] と [Notification Frequency] を設定します。
ステップ 4 [次へ（Next）] をクリックして続行します。

次のタスク

[Date And Time (NTP Server)]日付と時刻の設定 （41 ページ）に進みます。

日付と時刻の設定

次の手順では、Network Time Protocol（NTP）サーバを指定して日付と時刻を設定します。

ステップ 1 ナビゲーションペインで [Date and Time] をクリックします。

ステップ 2 [NTP Server(s)] に、NTP サーバの IP または NTP 名を入力します。

複数の NTP サーバがある場合は、スペースまたはカンマで区切ります。

ステップ 3 [Current System Time] および [Synchronize with Browser] フィールドは無視します。

ステップ 4 [次へ（Next）] をクリックして続行します。

次のタスク

[Configure Syslog]Syslog の設定 （41 ページ）に進みます。

Syslog の設定

[Syslog] 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 Syslog サーバの設定に使用されます。

ステップ 1 ナビゲーションペインで [Syslog] をクリックします。

ステップ 2 ページに情報をすべて入力し、[Next] をクリックして続行します。

詳細については、『*Cisco Threat Grid*アプライアンス管理者ガイド』を参照してください。

次のタスク

[Review and Install Configuration Settings]設定の確認とインストール （41 ページ）に進みます。

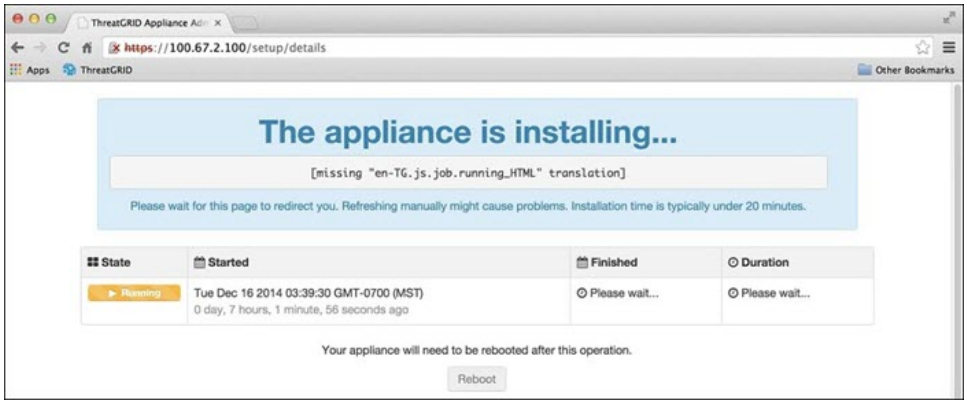
設定の確認とインストール

ワークフローの最後のステップでは、ネットワーク構成の設定を確認してインストールします。

ステップ 1 ナビゲーションペインで [Review And Install] をクリックし、次に [Start Installation] をクリックして、設定スクリプトのインストールを開始します。

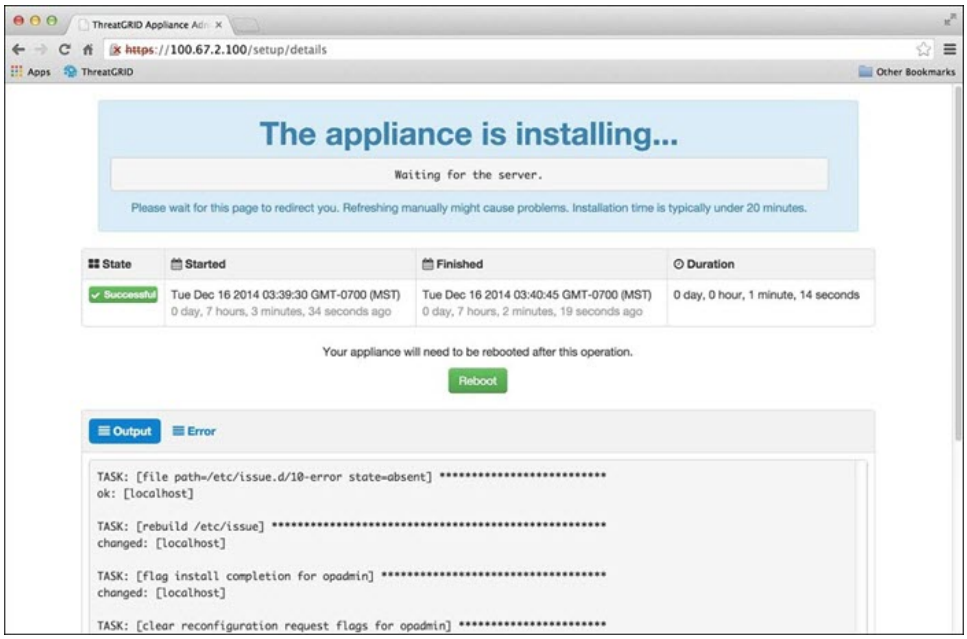
（注） インストールが完了するまでに10分以上かかる場合があります。この画面には、設定の適用状況に応じて設定情報が表示されます。

図 *21* : アプライアンスのインストール中



インストールが正常に完了すると、[State] が [Running] から [Successful] に変わり、[Reboot] ボタンが有効（緑色）になります。設定の出力も表示されます。

図 *22* : アプライアンスのインストール成功



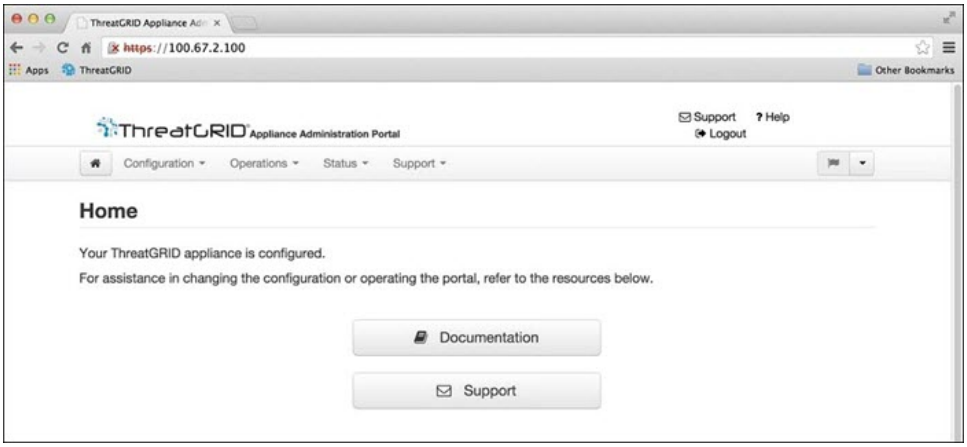
ステップ 2 [Reboot] をクリックします。

（注） リブートには最長 5 分かかることがあります。Threat Grid アプライアンスの再起動中は変更を行わないでください。

図 *23* : アプライアンス再起動中

リブート後に、Threat Grid アプライアンスが設定されたことを示すメッセージが**ホーム**ページに表示されます。

図 *24* : アプライアンスが正常に設定されました



これで設定プロセスは完了です。

Threat Grid アプライアンスの更新のインストール

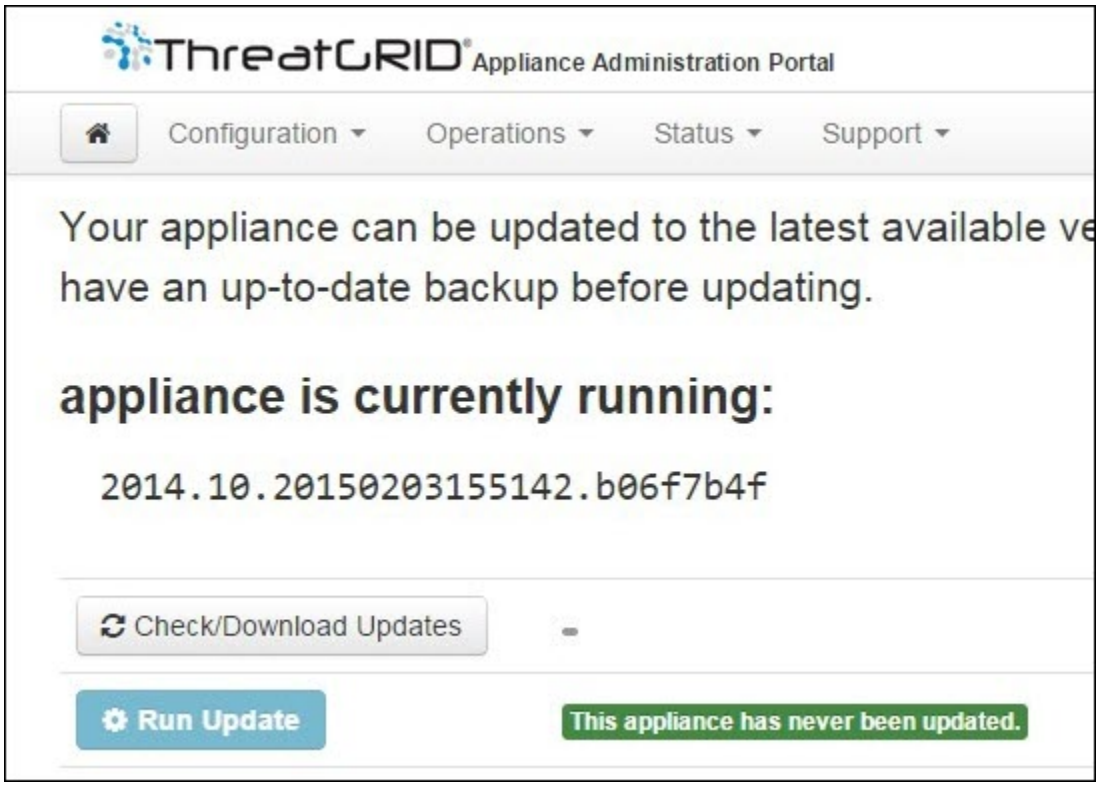
Threat Grid アプライアンスの初期設定の完了後は、作業を続ける前に、入手可能な更新をインストールすることをお勧めします。Threat Grid アプライアンスの更新は、OpAdmin Portal を使用して適用されます。

（注） 更新のインストールの詳細については、『*Cisco Threat Grid アプライアンス管理者ガイド*』を参照してください。

ステップ 1 まだ OpAdmin Portal にアクセスしていない場合は、ポータルにログインします。

ステップ 2 [Operations] メニューから、[Update Appliance] を選択して [Updates] ページを開きます。このページには、アプライアンスの現在のビルドが表示されます。

図 *25*：アプライアンスのビルド番号



（注） 対応するリリースバージョンについては、*Cisco Threat Grid* 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。

ステップ 3 [Check/Download Updates] をクリックします。

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がチェックされ、存在す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 4 更新のダウンロードが完了したら、[Run Update] をクリックしてインストールします。

アプライアンス設定のテスト

Threat Grid アプライアンスが現行のバージョンに更新されたら、Threat Grid にマルウェアサンプルを送信して、アプライアンスが正しく設定されていることをテストする必要があります。

ステップ 1 クリーンインターフェイスとして設定したアドレスを使用して、Threat Grid Portal にサインインします。

Threat Grid のログインページが開きます。

図 *26 : Threat Grid Portal* のログイン

ステップ 2 次のデフォルトの資格情報を入力します。

- ログイン：**admin**
- **パスワード** ：opadmin の構成ワークフローの最初のステップで入力した新しいパスワードを使用します。パスワードは、適時変更することをお勧めします。

ステップ 3 [Login] をクリックすると、[Threat Grid Sample Analysis] ページが開きます。

ステップ 4 右上隅の [Submit a Sample] ボックスで、サンプルファイルを選択するか、マルウェア分析用に送信する URL を入力します。

ステップ 5 [Upload Sample] をクリックします。

Threat Grid のサンプル分析プロセスが起動します。サンプルの分析は複数の段階を通じて進むことがわかります。分析中、サンプルは [Submissions] セクションに表示されます。分析が完了すると、結果は [Analysis Report] の詳細とともに、[Samples] セクションに示されます。

次のタスク

Threat Grid アプライアンスが設定され、初期設定が完了したら、アプライアンス管理者は、SSL 証明書の管理やユーザの追加などのその他のタスクを実行できます。管理者タスクの詳細については、『*Cisco Threat Grid アプライアンス管理者ガイド*』を参照してください。