



Cisco Threat Grid アプライアンスバージョン 2.10 設定および構成ガイド

初版：2020年1月28日

最終更新：2020年4月10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。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2020 Cisco Systems, Inc. All rights reserved.



目次

第 1 章

はじめに 1

Cisco Threat Grid アプライアンスについて 1

このリリースの最新情報 2

対象読者 2

製品に関する資料 2

Threat Grid のサポート 3

サポート モードの有効化 6

サポート スナップショット 6

第 2 章

計画 9

対応ブラウザ 9

環境要件 10

ハードウェア要件 10

ネットワーク要件 11

DNS サーバアクセス 12

NTP サーバアクセス 12

統合 12

DHCP 12

ライセンス 12

レート制限 12

組織とユーザ 13

変更点 (Updates) 13

ユーザ インターフェイス 13

TGSH ダイアログ 14

Threat Grid シェル (tgsh)	14
OpAdmin Portal	14
Threat Grid Portal	15
ネットワーク インターフェイス	15
ネットワーク インターフェイスの設定図	17
ファイアウォール ルール	18
ログイン名とパスワード (デフォルト)	22
設定と構成の概要	22
<hr/>	
第 3 章	初期ネットワーク設定 25
	アプライアンスの電源オンと起動 25
	TGSH ダイアログを使用したネットワークの設定 27
<hr/>	
第 4 章	OpAdmin Portal の設定 33
	はじめに 33
	OpAdmin ポータルにログインする 34
	管理者パスワードの変更 35
	エンドユーザライセンス契約書の確認 35
	Configuration Wizard 35
	ネットワークの設定 36
	ライセンスのインストール 36
	NFS の設定 38
	電子メールホストの設定 39
	通知の設定 40
	日付と時刻の設定 41
	Syslog の設定 41
	設定の確認とインストール 41
	Threat Grid アプライアンスの更新のインストール 43
	アプライアンス設定のテスト 44



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マニュアル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 \(1 ページ\)](#)
- [このリリースの最新情報 \(2 ページ\)](#)
- [対象読者 \(2 ページ\)](#)
- [製品に関する資料 \(2 ページ\)](#)
- [Threat Grid のサポート \(3 ページ\)](#)

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、安全かつ高度にセキュリティ保護された、オンプレミスの高度なマルウェア分析を提供し、詳細な脅威分析およびコンテンツを使用します。Threat Grid アプライアンスは、完全な Threat Grid マルウェア分析プラットフォームを提供し、Cisco Threat Grid M5 アプライアンスサーバ (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「サーバのセットアップ」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 2.10 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 2.10 における変更: 2020 年 1 月 28 日

機能または更新	セクション
RADIUS 認証のサポートが追加されました。	ユーザ インターフェイス ネットワーク インターフェイス ファイアウォールルール

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 アプライアンスのセットアップおよび設定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 ロックアップ 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 Appliance 製品マニュアルは、[Threat grid の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

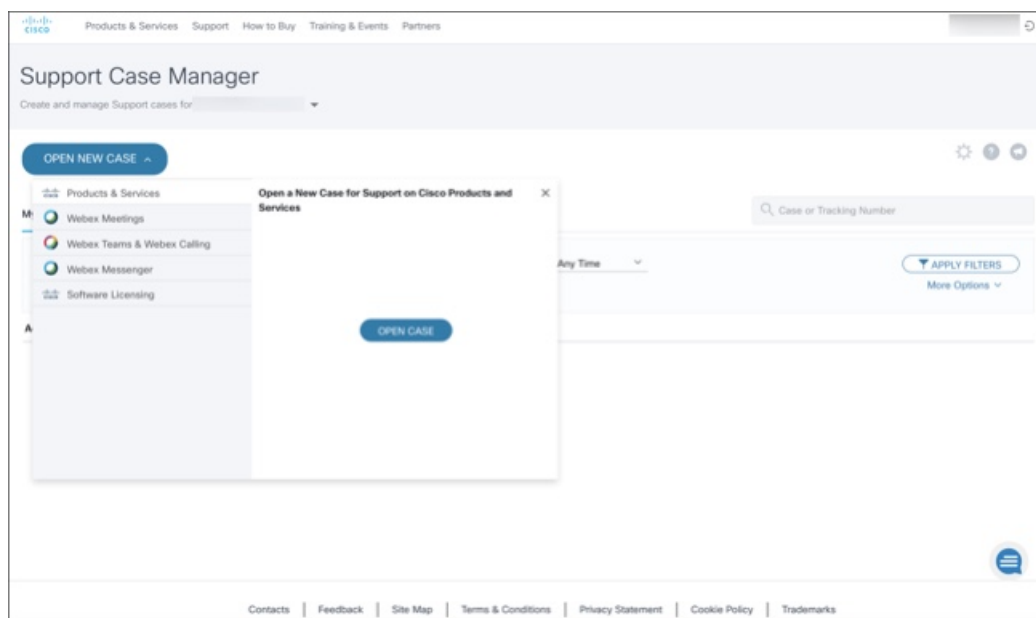
リリースノート、Threat Grid オンラインヘルプ、API ドキュメント、およびその他の情報を含む Threat Grid Portal ユーザドキュメントは、ユーザインターフェイス上部のナビゲーションバーにある [Help] メニューから入手できます。

Threat Grid のサポート

Threat Grid に関するご質問やサポートが必要な場合は、<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。

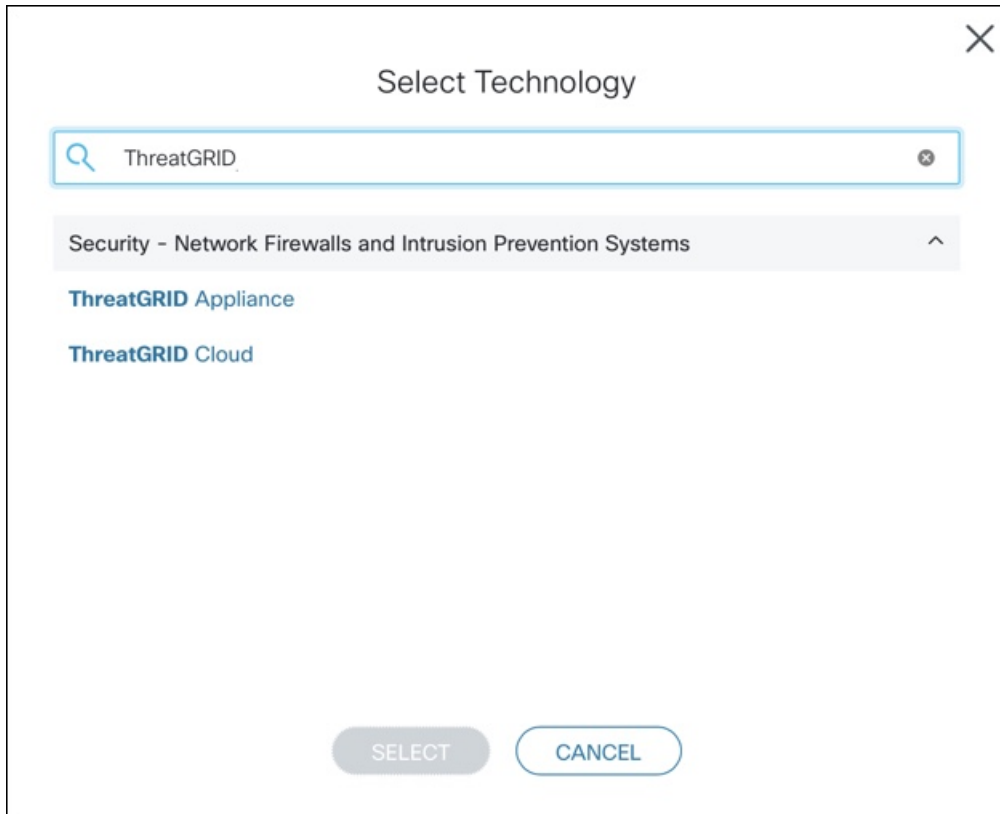
図 2: エンタイトルメントのチェック

The screenshot shows the 'Support Case Manager' interface. At the top, there are navigation links: Products & Services, Support, How to Buy, Training & Events, and Partners. The main heading is 'Support Case Manager' with a sub-heading 'Open a new support case for'. Below this is a breadcrumb trail: 'OPEN NEW CASE Products & Services'. A progress indicator shows three steps: 1. Check Entitlement (active), 2. Describe Problem, and 3. Review & Submit. The 'Request Type' section has three radio buttons: 'Diagnose and Fix', 'Request RMA', and 'Ask a Question' (selected). Below this are two dropdown menus: 'Find Product by Serial Number' and 'Find Product by Service Agreement'. The 'Bypass Entitlement' section has a dropdown menu with 'CPR / Contract data not in C3' selected. At the bottom, there is a blue 'NEXT' button and a 'Save draft and exit' link.

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 リストからサーバを選択して [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>)
- <https://www.cisco.com/c/en/us/support/index.html> にあるシスコサポート & ダウンロードのメインページを参照してください :

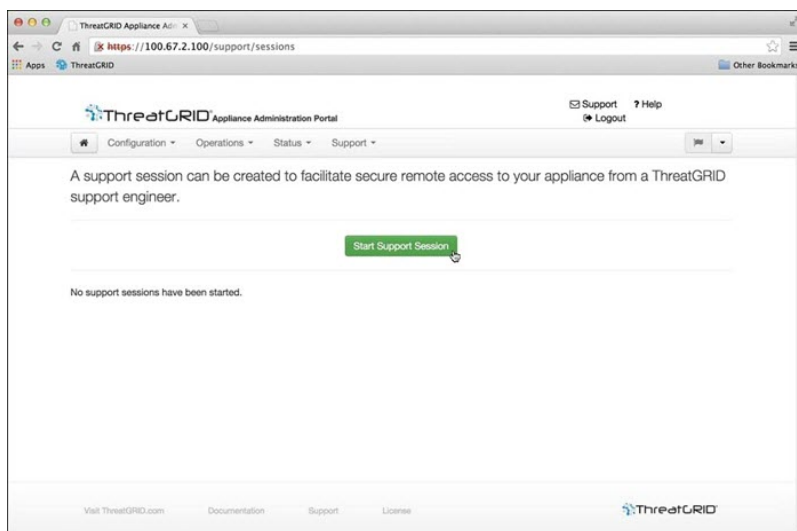
サポート モードの有効化

Threat Grid のエンジニアからのサポートが必要なときに、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、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アクセス権が付与されます。アプライアンスの通常の動作には影響しません。

OpAdmin ポータルの [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。TGSH ダイアログ、レガシーの Face Portal UI から有効にするか、リカバリモードで起動する際に有効にすることもできます。

ステップ 1 OpAdmin ポータルで [Support] メニューをクリックして、[Live Support Session] を選択します。

図 4: OpAdmin で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、ライセンスの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。

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] をクリックして、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信したら、オンプレミスのネットワーク環境に合わせてセットアップし、設定する必要があります。

この章には、設定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 \(9 ページ\)](#)
- [環境要件 \(10 ページ\)](#)
- [ハードウェア要件 \(10 ページ\)](#)
- [ネットワーク要件 \(11 ページ\)](#)
- [DNS サーバアクセス \(12 ページ\)](#)
- [NTP サーバアクセス \(12 ページ\)](#)
- [統合 \(12 ページ\)](#)
- [DHCP \(12 ページ\)](#)
- [ライセンス \(12 ページ\)](#)
- [組織とユーザ \(13 ページ\)](#)
- [変更点 \(Updates\) \(13 ページ\)](#)
- [ユーザ インターフェイス \(13 ページ\)](#)
- [ネットワーク インターフェイス \(15 ページ\)](#)
- [ファイアウォールルール \(18 ページ\)](#)
- [ログイン名とパスワード \(デフォルト\) \(22 ページ\)](#)
- [設定と構成の概要 \(22 ページ\)](#)

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+ ポートがないか、または SFP+ が望ましくなければ、1000Base-T のトランシーバを使用できます (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)。

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、(UCS C220-M3 および C220-M4 サーバ上で) リモート KVMを使用できます。



(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。

[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（要求）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) Clean network 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。

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）
 - 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（マルウェアトラフィックを含む）からの発信トラフィックに使用されます。



(注) 内部ネットワークの評価を保護するために、社内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セットアップおよび設定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（「[ThreatGrid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 Dialog および OpAdmin で使用できます。RADIUS 認証は、Threat Grid 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。

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。Threat Grid アプライアンスが正常に起動すると、[TGSH] ダイアログが表示されます。

TGSH ダイアログへの再接続

[TGSH] ダイアログはコンソール上で開いたままになり、アプライアンスにモニタを接続するか、またはリモート KVM 経由で CIMC が設定されている場合は、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、(estroy-data や forced backup などの) コマンド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 ユーザと同じクレデンシャルを使用するため、tgsh を介して行われたパスワードの変更/更新は 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	<ul style="list-style-type: none"> 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 SSH (inbound) for TGSH Dialog バックアップとクラスタリングのための NFSv4 (アウトバウンド) 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、管理ポートを抜くと、機能していない (または機能が非常に高い) Threat Grid アプライアンスになります。 <p>(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。</p>
クラスタ	<p>非管理 SFP+ ポートはクラスタリングに使用されます。</p> <ul style="list-style-type: none"> 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)]	<ul style="list-style-type: none">• 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 (inbound for TGSH Dialog)• 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)• RADIUS (発信)

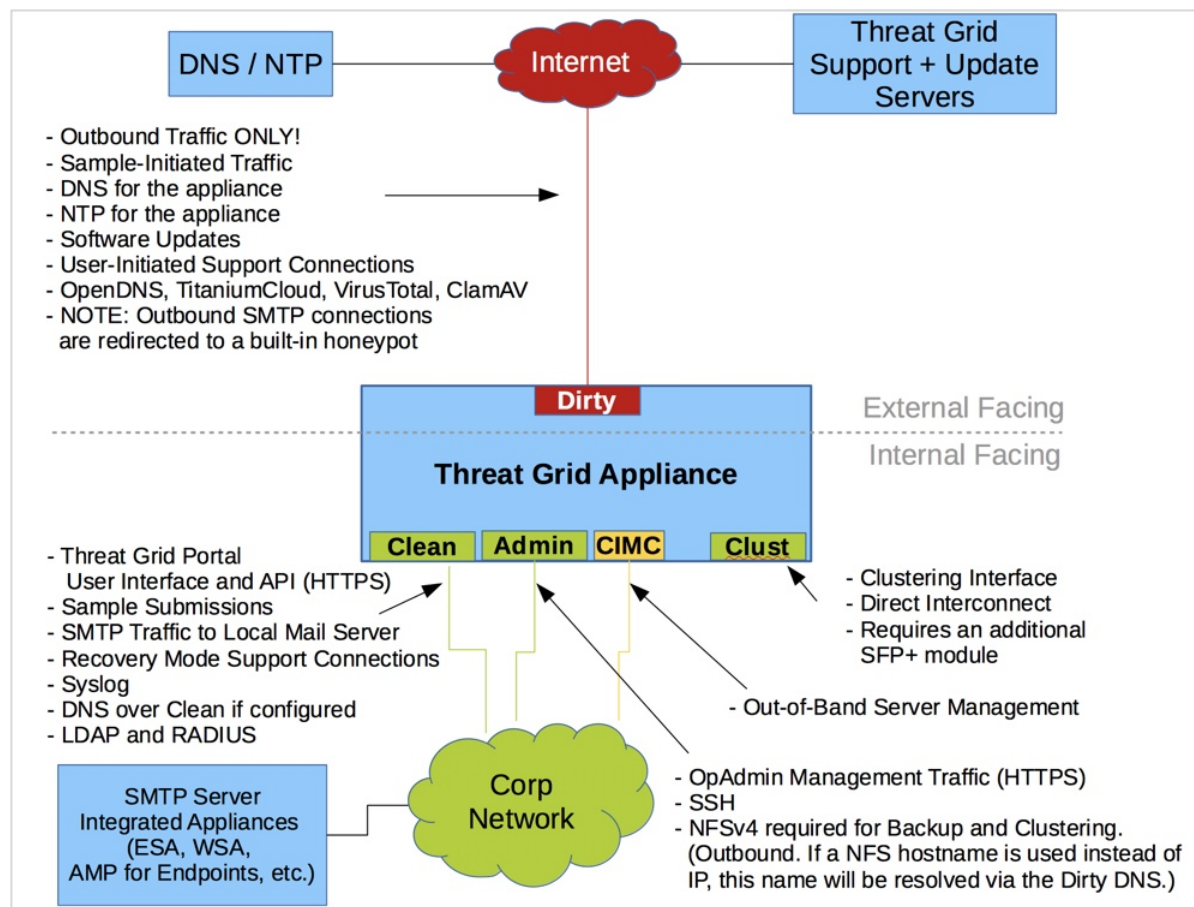
インターフェイス	説明
ダーティ	<p>ダーティネットワークに接続します。インターネットアクセスが必要です。発信のみ。</p> <p>プライベート IP に送信されるトラフィックは、ネットワーク出口のローカリゼーションファイアウォールでドロップされるため、ダーティインターフェイスには独自の DNS（プライベート IP）を使用しないようにしてください。</p> <ul style="list-style-type: none"> • DNS <ul style="list-style-type: none"> (注) AMP for Endpoints プライベートクラウドとの統合を設定し、AMP 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 <p>(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。</p>
CIMC インターフェイス	<p>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。</p> <p>(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。</p>

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応

じて、ダーティインターフェイスを内部に接続するか、適切なネットワークセキュリティ対策を講じてクリーンインターフェイスを外部に接続するかを決定できます。

図 6: ネットワークインターフェイス設定図



(注) Threat Grid アプライアンス (v2.7.2 以降) では、**enable_clean_interface** オプションは使用できませんが、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) により、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にアクセスできます。

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	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	LDAP サーバ	TCP	636	許可 (Allow)	任意。LDAP 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	RADIUS サーバ	DTLS	2083	許可	Threat Grid 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 ユーザーインターフェイス。
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。

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	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。

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 ポータル 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、独立した状態になります。
CIMC	Login: admin Password: password

設定と構成の概要

このドキュメントでは、次のセットアップおよび初期設定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
- アプライアンスのセットアップのテスト

『[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、（ライセンスのインストール、電子メールサーバ、SSL 証明書などの）残りの管理設定タスクを完了します。

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

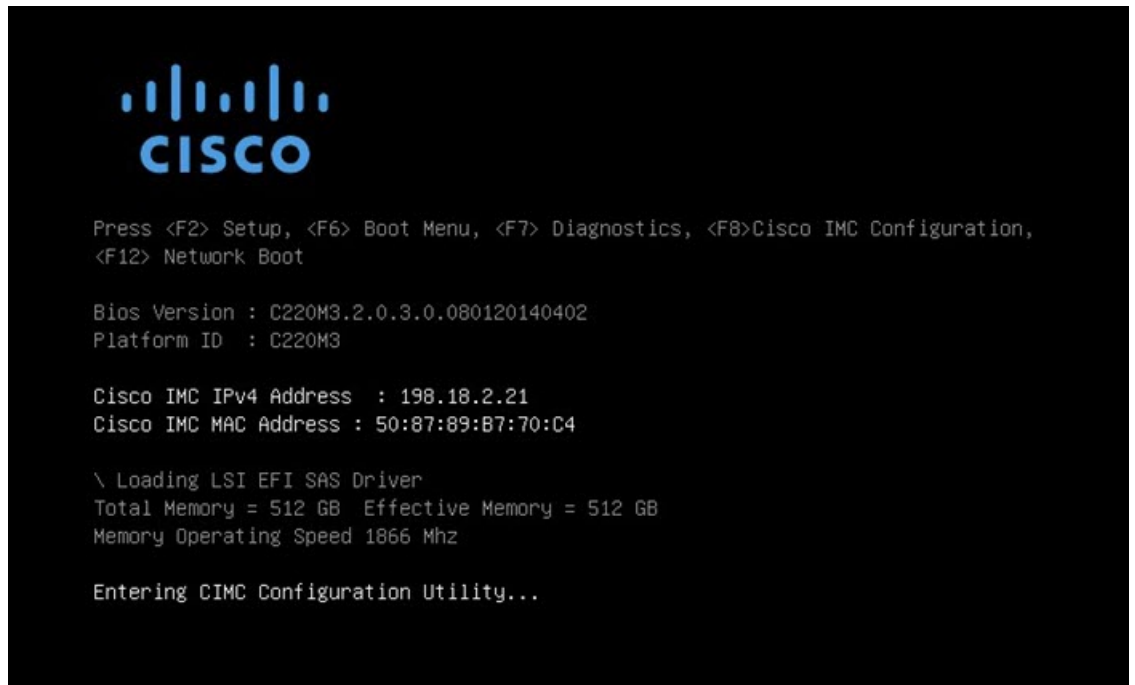
この章では、TGSH ダイアログを使用してネットワークの初期設定を完了する手順について説明します。内容は次のとおりです。

- [アプライアンスの電源オンと起動 \(25 ページ\)](#)
- [TGSH ダイアログを使用したネットワークの設定 \(27 ページ\)](#)

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

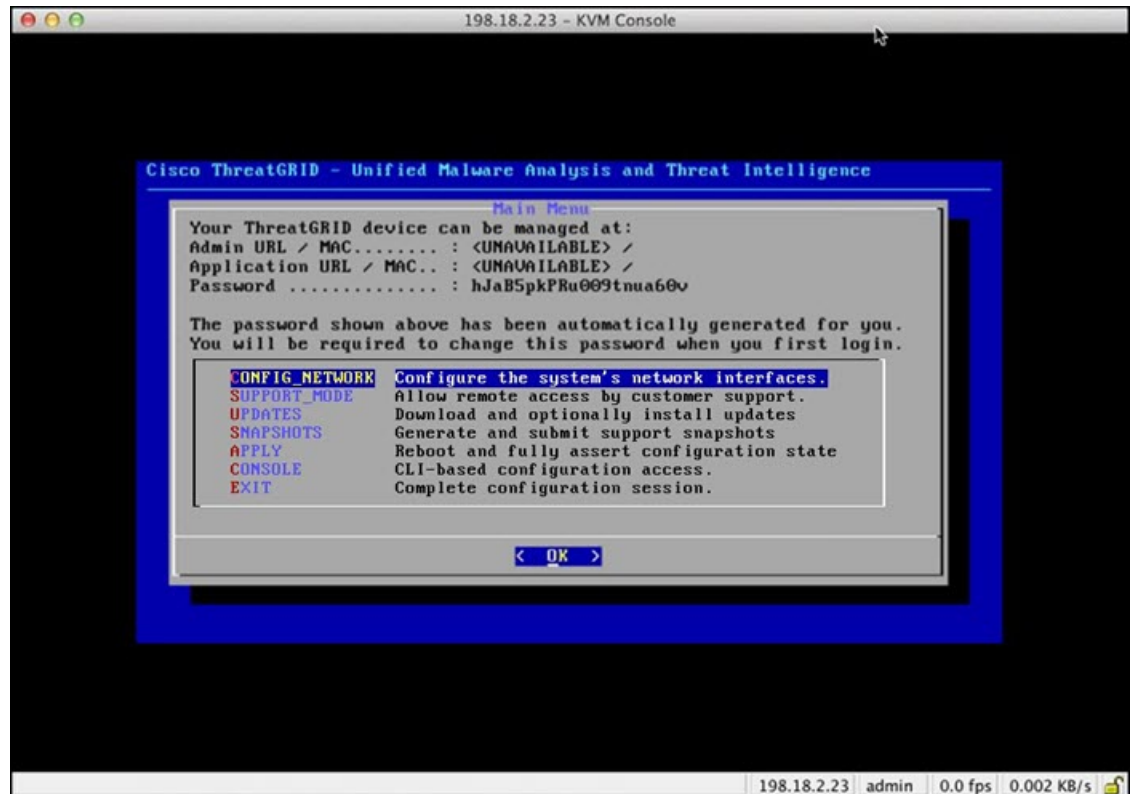




- (注) このインターフェイスを設定する場合は、メモリチェックが完了した後に **F8** を押します。
『Cisco Threat Grid アプライアンス管理者ガイド』の付録「CIMC の設定」を参照してください。

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、この後の設定手順で 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設定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

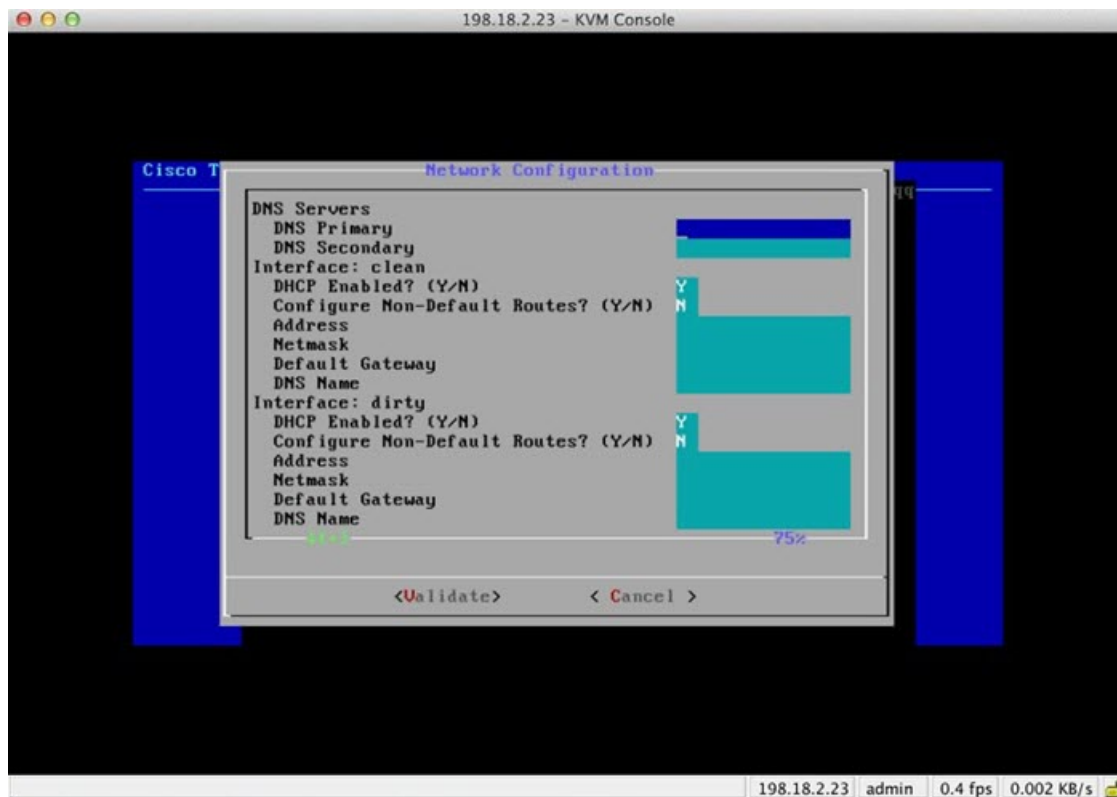
初期ネットワーク設定は、TGSH ダイアログで行います。基本設定が完了すると、OpAdmin ポータルへのアクセスが許可されます。このポータルでは、追加の設定タスクを実行できません。



- (注) DHCP ユーザの場合、次の手順では、スタティック IP アドレスを使用していることを前提としています。DHCP を使用して IP を取得している場合、詳細については、『[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には、古い文字をバックスペースに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）

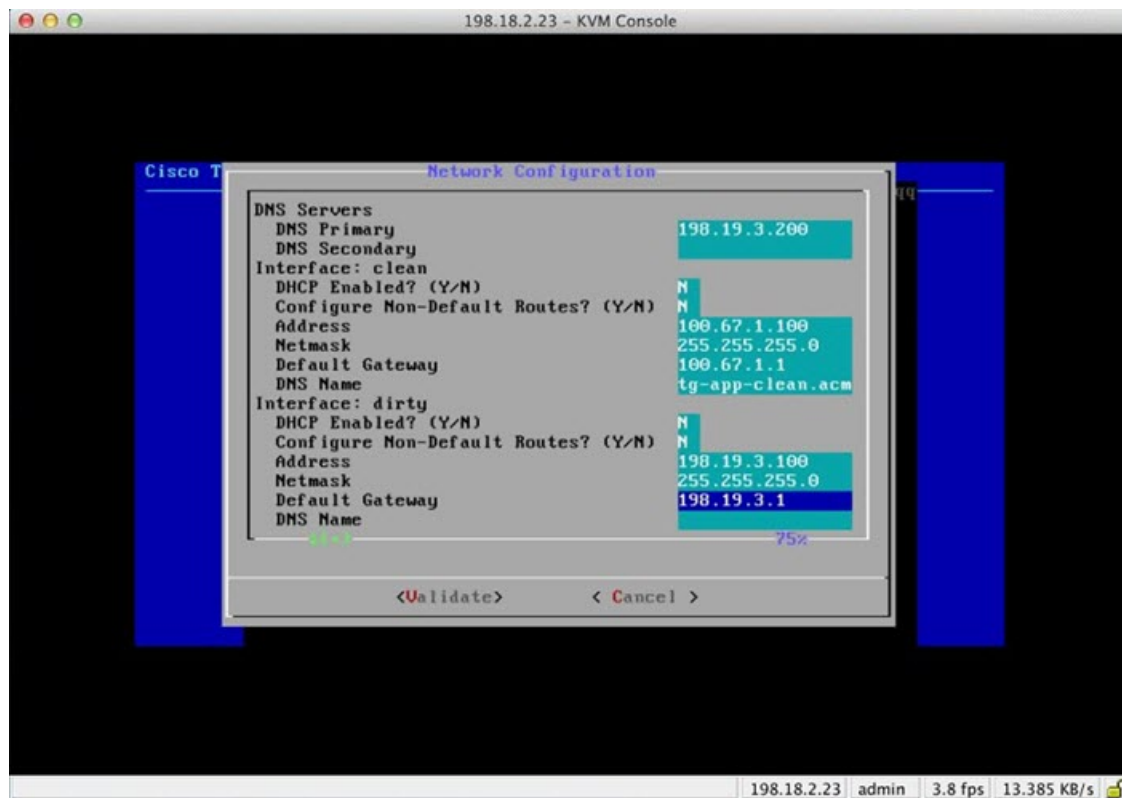
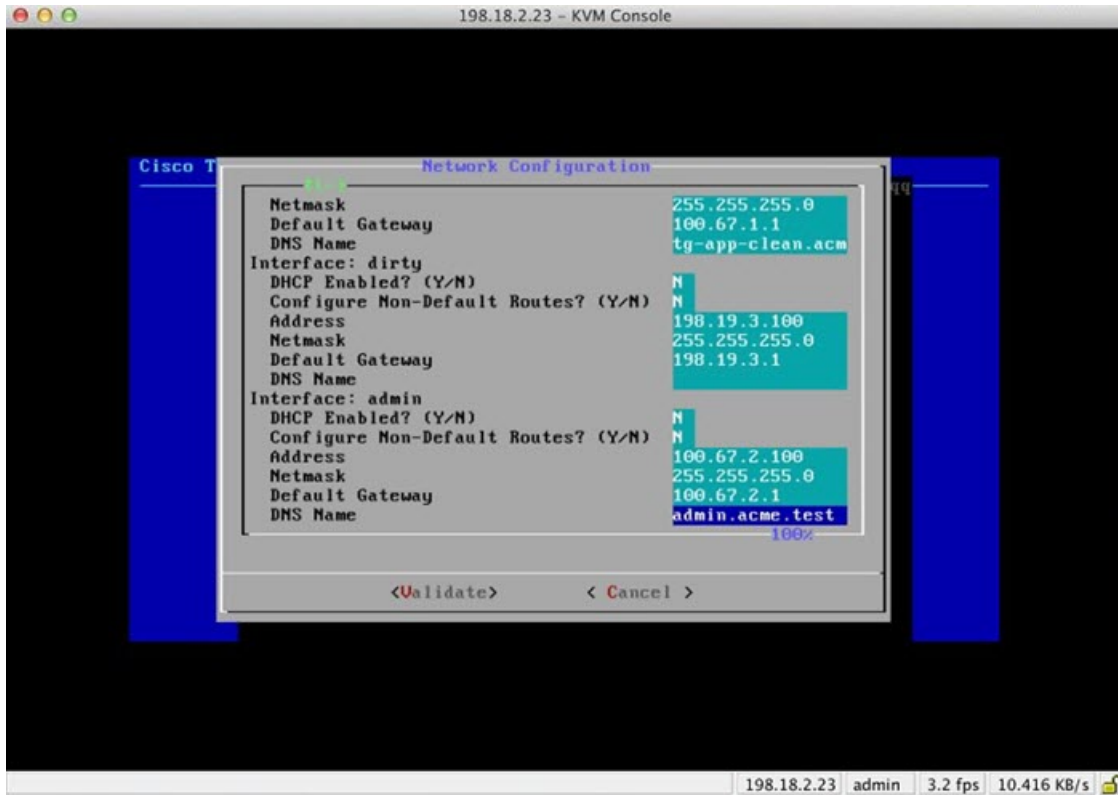


図 11: 進行中のネットワーク設定 (管理者)

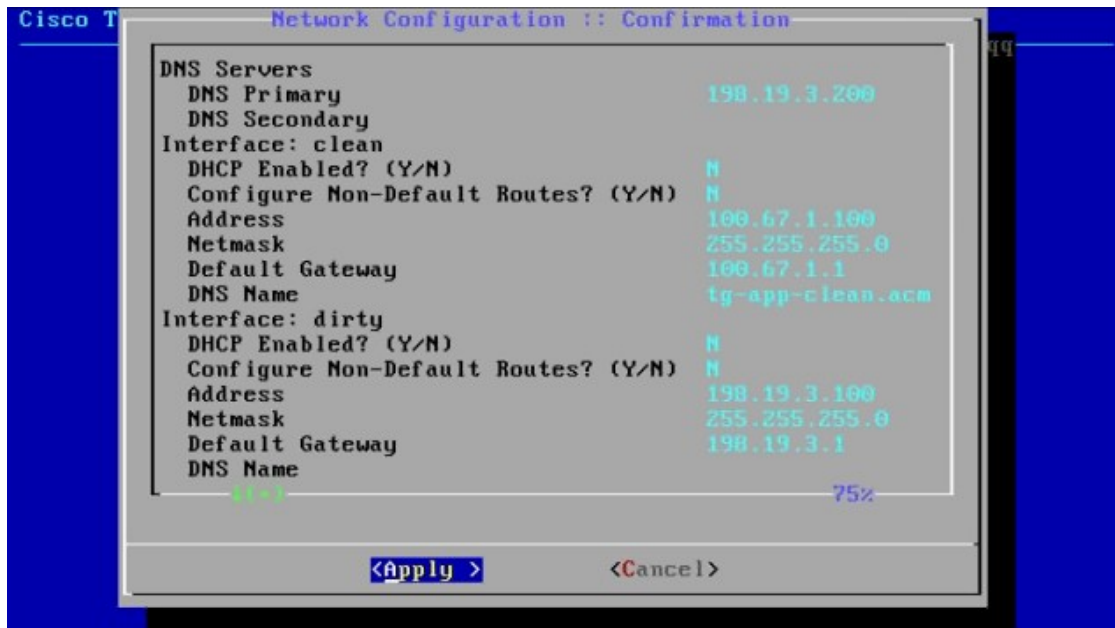


ステップ7 すべてのネットワーク設定を入力したら、Tab キーで下に移動し、[Validate] を選択して入力内容を検証します。

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。

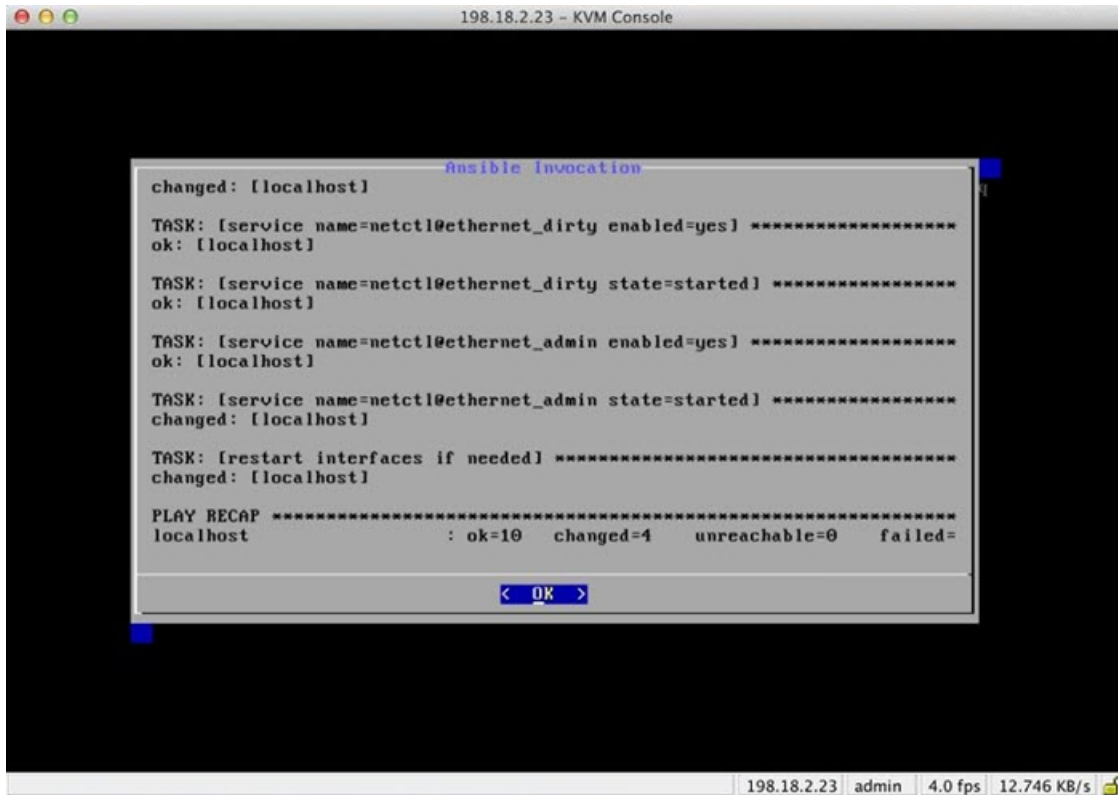
図 12: ネットワーク構成の確認



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



The screenshot shows a KVM console window titled "198.18.2.23 - KVM Console". Inside the window, a terminal window displays the output of an Ansible invocation. The output includes the following text:

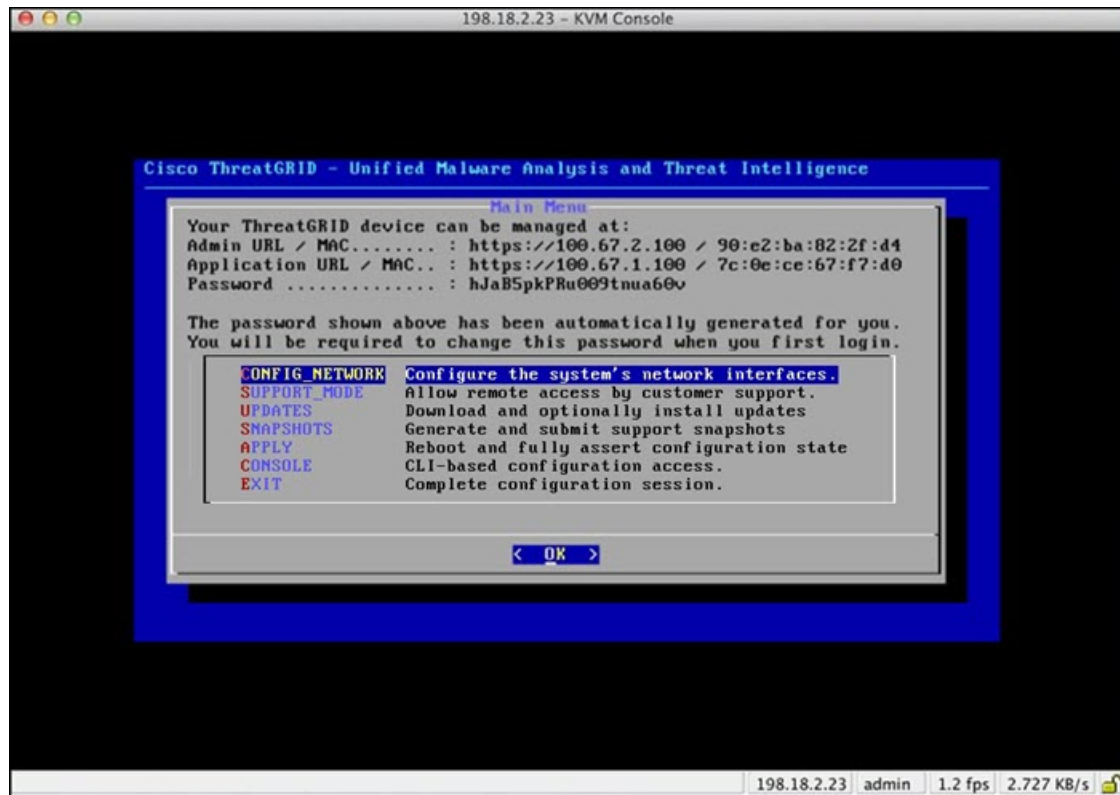
```
changed: [localhost]
TASK: [service name=netctl@ethernet_dirty enabled=yes] *****
ok: [localhost]
TASK: [service name=netctl@ethernet_dirty state=started] *****
ok: [localhost]
TASK: [service name=netctl@ethernet_admin enabled=yes] *****
ok: [localhost]
TASK: [service name=netctl@ethernet_admin state=started] *****
changed: [localhost]
TASK: [restart interfaces if needed] *****
changed: [localhost]
PLAY RECAP *****
localhost      : ok=10  changed=4  unreachable=0  failed=
```

At the bottom of the terminal window, there is a blue button labeled "< OK >". The console window's status bar at the bottom right shows "198.18.2.23 | admin | 4.0 fps | 12.746 KB/s | 🔒".

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 \(33 ページ\)](#)
- [Configuration Wizard \(35 ページ\)](#)
- [Threat Grid アプライアンスの更新のインストール \(43 ページ\)](#)
- [アプライアンス設定のテスト \(44 ページ\)](#)

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
- (ウィザードを使用して設定されていない) ネットワーク構成設定の確認
- 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。

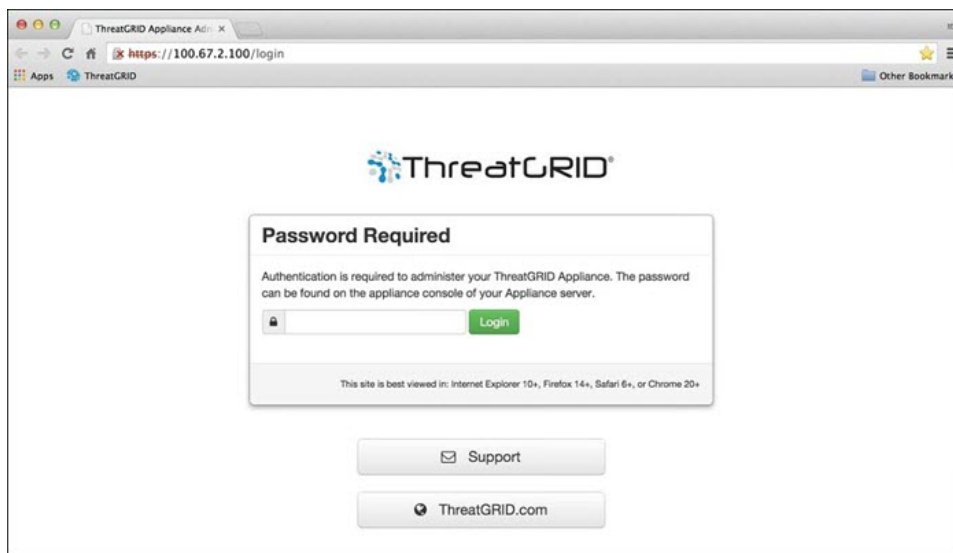
OpAdmin ポータルにログインする

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 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（これはテキストファイルに保存する必要があります）。

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 Agreement] [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、Threat Grid アプライアンスの設定を行います。

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] 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」の項に記載されている手順を実行します。

次のタスク

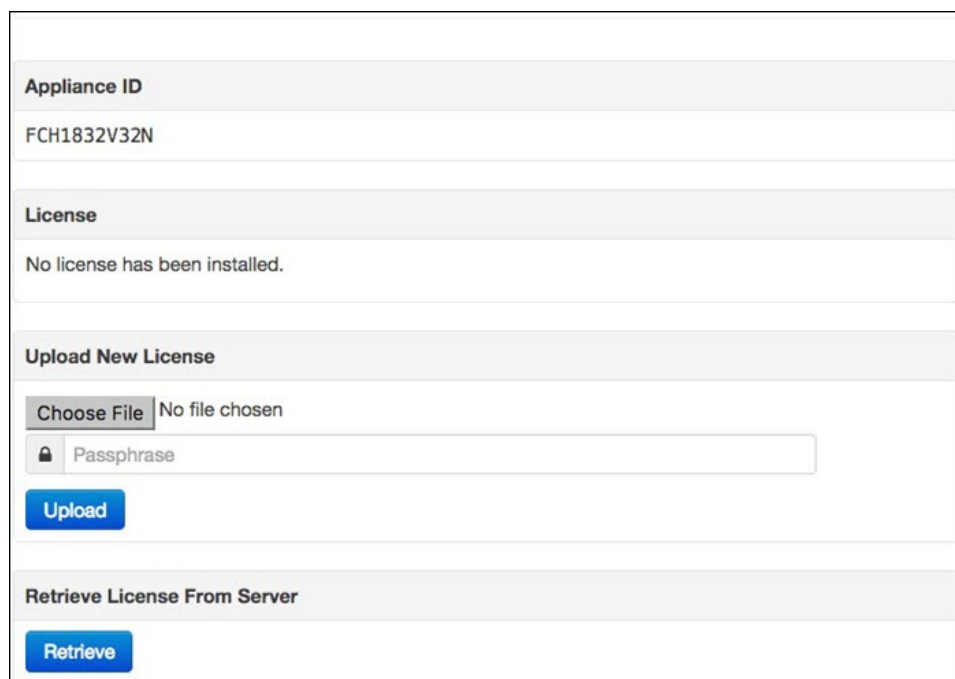
[Install License][ライセンスのインストール \(36 ページ\)](#) に進みます。

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



The screenshot shows the 'License' section of the Threat Grid Appliance configuration page. It includes the following elements:

- Appliance ID:** FCH1832V32N
- License:** No license has been installed.
- Upload New License:**
 - A file selection button labeled 'Choose File' with the text 'No file chosen' next to it.
 - A password field labeled 'Passphrase' with a lock icon on the left.
 - An 'Upload' button.
- Retrieve License From Server:**
 - A 'Retrieve' button.

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。アプライアンスをインストールするときに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

The screenshot displays the license management interface. At the top, the 'Appliance ID' is shown as 'FCH1832V32N'. Below this is a table for license details:

License	
Licensee	No Name Provided provision@threatgrid.com
Business	2f518e6d-dd45-4397-9533-3c6d38239c32
Validity	Fri, 22 Sep 2017 14:47:46 +0000 - Mon, 21 Sep 2020 14:47:46 +0000
Product SKU	
Daily Submissions	1500

Below the table are two main sections:

- Upload New License:** Includes a 'Choose File' button (currently showing 'No file chosen'), a 'Passphrase' input field with a lock icon, and an 'Upload' button.
- Retrieve License From Server:** Includes a 'Retrieve' button.

A green 'Next >' button is located at the bottom right of the interface.

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。

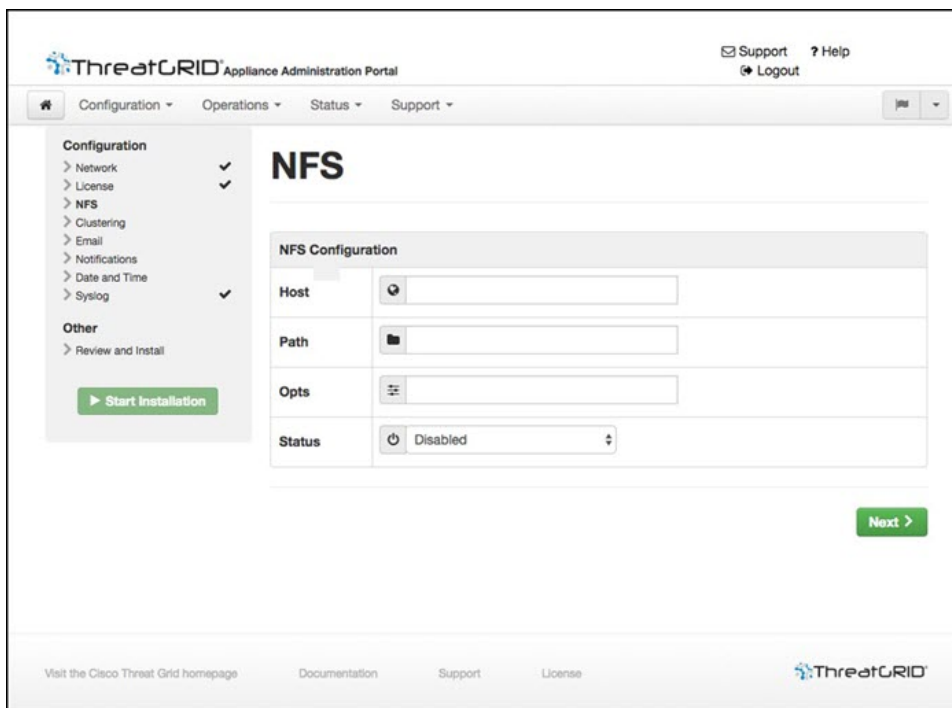
NFS の設定

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] : ファイルが保存される NFS ホストサーバ上のロケーションへの絶対パス。
- [Oopts] : 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 (保留キー)。

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せん。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

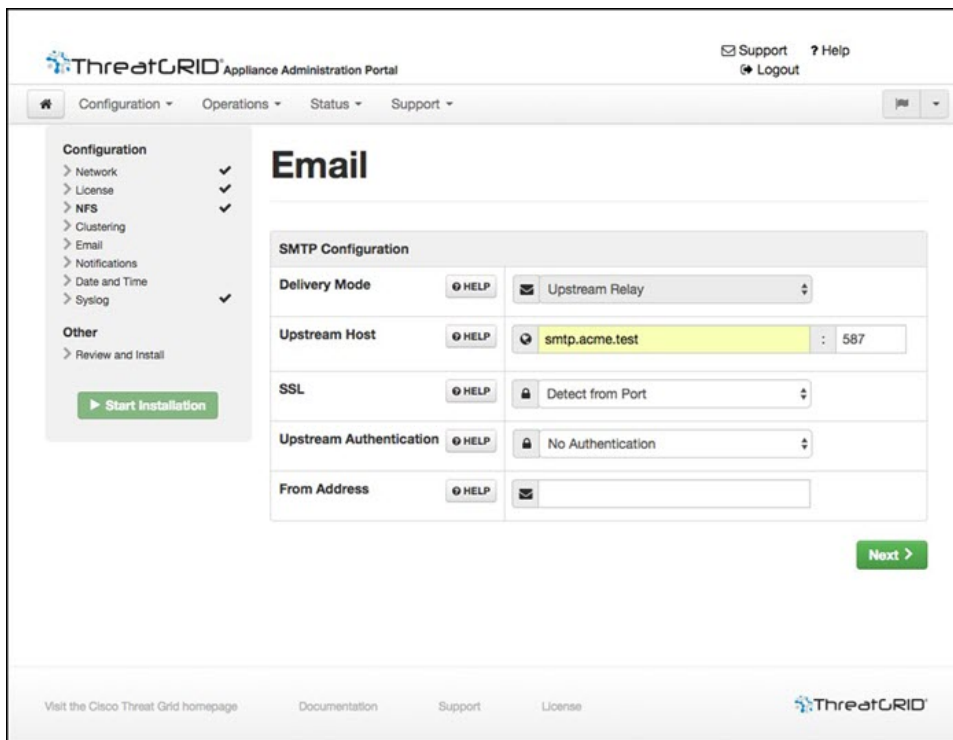
[Configure Email Host] [電子メールホストの設定 \(39 ページ\)](#) に進みます。

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

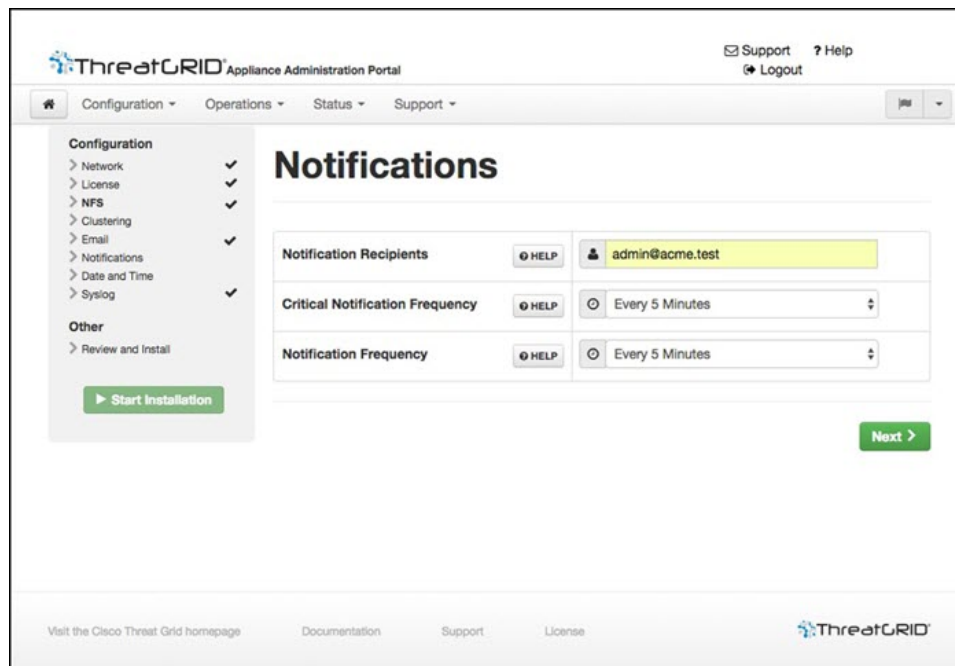
[Configure Notifications] [通知の設定 \(40 ページ\)](#) に進みます。

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。

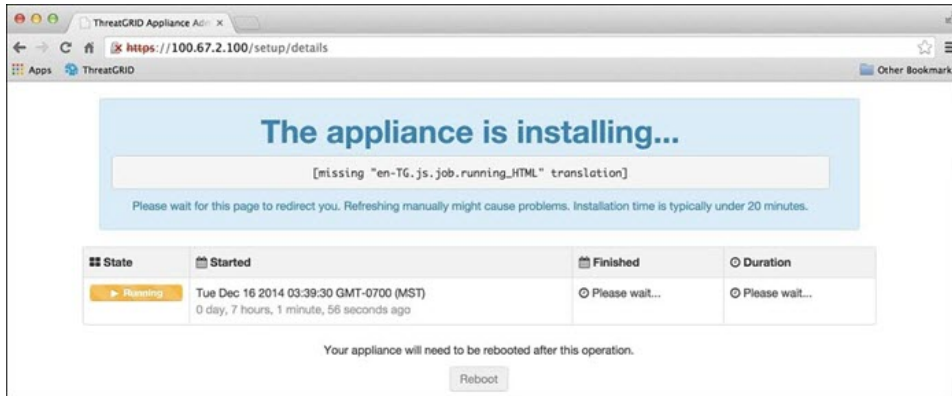
設定の確認とインストール

ワークフローの最後のステップは、ネットワーク構成の設定を確認してインストールすることです。

-
- ステップ 1 [Navigation] 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。

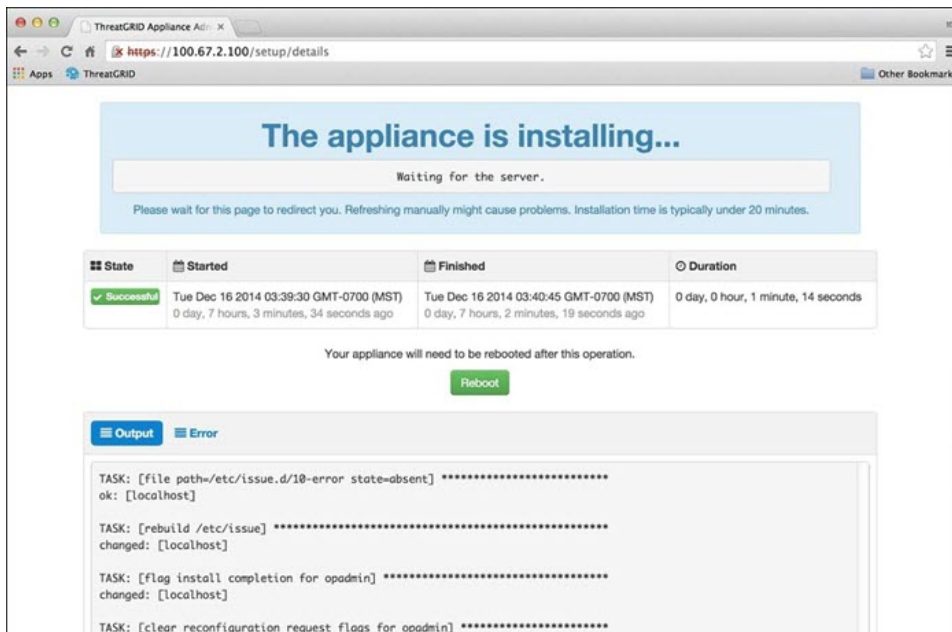
(注) インストールが完了するまでに10分以上かかる場合があります。この画面には、設定の適用状況に応じて設定情報が表示されます。

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（緑色）が有効になります。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。

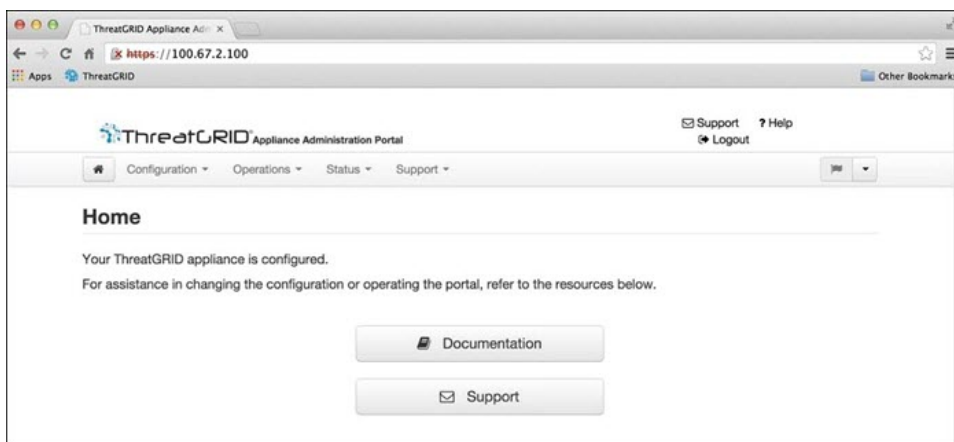
(注) リポートには最長 5 分かかることがあります。Threat Grid アプライアンスの再起動中は変更しないでください。

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、入手可能な更新プログラム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。

エアギャップ実装を使用しているユーザは、[Threat Grid のサポート](#)に連絡して、ダウンロード可能な更新ブートイメージを入手することができます。

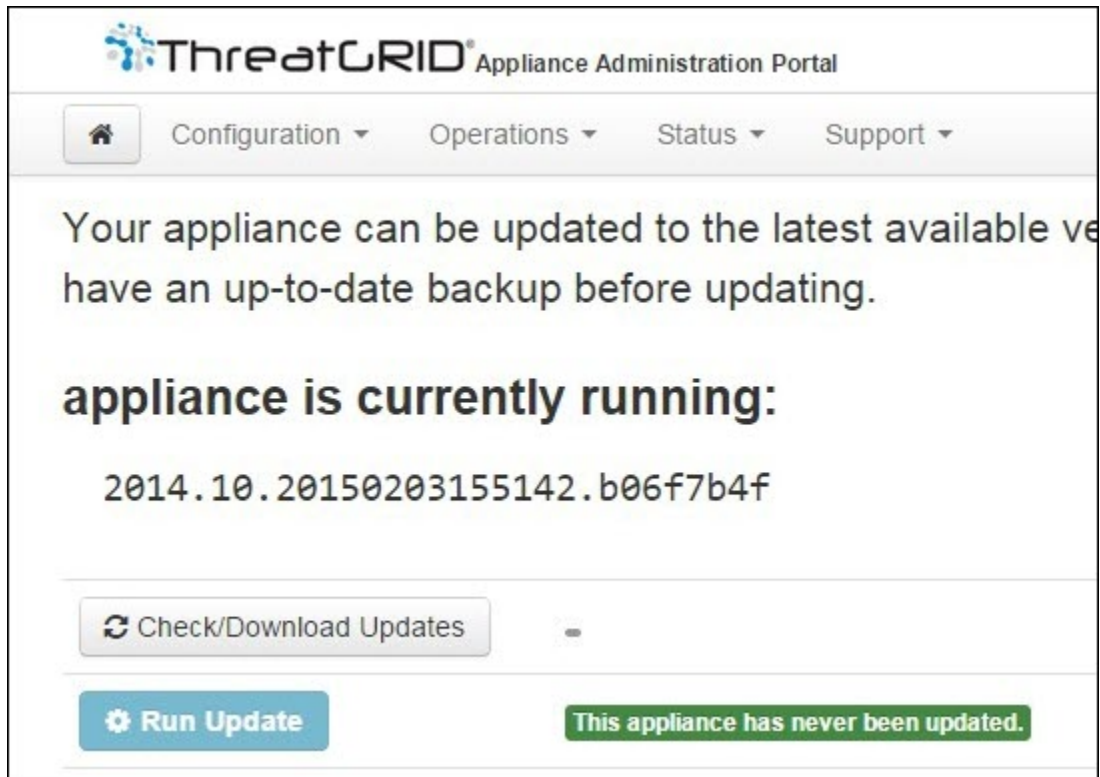


- (注) 更新のインストールの詳細については、『[Cisco Threat Grid アプライアンス管理者ガイド](#)』を参照してください。

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。

Threat Grid 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ているかどうかを確認し、その場合はダウンロードします。これには少し時間がかかる場合があります。

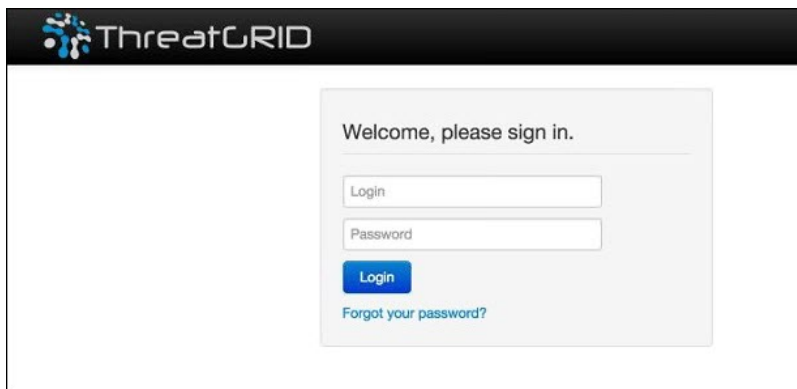
ステップ4 更新のダウンロードが完了したら、[Run Update] をクリックしてインストールします。

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 ポータルのログイン



- 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 の設定ワークフローにおける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。

