



Cisco Secure Malware Analytics アプライアンスバージョン2.19 スタートアップガイド

最終更新：2025年1月27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 –2024 Cisco Systems, Inc. All rights reserved.



目次

第 1 章

はじめに 1

Cisco Secure Malware Analytics アプライアンスについて 1

対象読者 2

前提条件 2

製品に関する資料 2

このリリースの最新情報 3

サポートされるブラウザ 3

更新 4

サポート 4

設定と構成の概要 7

第 2 章

初期ネットワーク設定 9

アプライアンスの電源オンと起動 9

管理 TUI を使用したネットワークの設定 10

第 3 章

管理 UI の設定 13

はじめに 13

管理 UI へのログイン 14

管理者パスワードの変更 15

エンドユーザーライセンス契約書の確認 16

設定ウィザード 16

Home 17

ネットワークの設定 17

NFS の設定 18

クラスタリングの設定	20
最初のクラスタノードの設定	21
追加のクラスタノードへの結合	21
ライセンスのインストール	22
電子メールの設定	24
通知の設定	25
日付と時刻の設定	26
システムログの設定	27
設定の確認とインストール	27
Cisco Secure Malware Analytics アプライアンスの更新をインストールする	30
アプライアンス設定のテスト	31



第 1 章

はじめに

この章では、Cisco Secure Malware Analytics 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 Secure Malware Analytics アプライアンスについて \(1 ページ\)](#)
- [対象読者 \(2 ページ\)](#)
- [前提条件 \(2 ページ\)](#)
- [製品に関する資料 \(2 ページ\)](#)
- [このリリースの最新情報 \(3 ページ\)](#)
- [サポートされるブラウザ \(3 ページ\)](#)
- [更新 \(4 ページ\)](#)
- [サポート \(4 ページ\)](#)
- [設定と構成の概要 \(7 ページ\)](#)

Cisco Secure Malware Analytics アプライアンスについて

Cisco 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 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。手順については、『*Cisco Secure Malware Analytics Appliance Setup and Configuration Guide*』（バージョン 2.7 以前）のサーバー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。

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 Cisco Secure Malware Analytics 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、マルウェアのサンプルを分析に送信するまでを対象とした、新しい Cisco Secure Malware Analytics アプライアンスの初期設定および構成を完了する方法について説明します。

前提条件

『[Cisco Secure Malware Analytics Appliance Administration Guide](#)』で説明されているように、必要な情報を収集し、計画手順を完了していることを前提としています。

また、『[Cisco Secure Malware Analytics M5 Hardware Installation Guide](#)』の指示に基づいて、Cisco Secure Malware Analytics アプライアンスをすでにセットアップしていることも前提としています。

これら2つのタスクをまだ完了していない場合は、このスタートガイドで説明されている手順を開始する前に完了してください。

製品に関する資料

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。

- [Cisco Secure Malware Analytics Appliance Release Notes](#)
- [Cisco Secure Malware Analytics Version Lookup Table](#)
- [Cisco Secure Malware Analytics Appliance Administration Guide](#)

- [Cisco Secure Malware Analytics M5 Hardware Installation Guide](#)



(注) Cisco Secure Malware Analytics M5 アプライアンスは、Cisco Secure Malware Analytics 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) Cisco Secure Malware Analytics アプライアンスの以前のバージョンの製品ドキュメントは、[Cisco Secure Malware Analytics](#) のインストールとアップグレードにあります。

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、ユーザーインターフェイス上部のナビゲーションバーにある [ヘルプ (Help)] メニューから入手できます。

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 リリースの変更点

機能または更新	セクション
管理 UI のダッシュボードの機能強化	Home (17 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。	

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はサポートされません。

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。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（「[Cisco Secure Malware Analytics アプライアンスの更新をインストールする](#)」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、順に実行する必要があります。

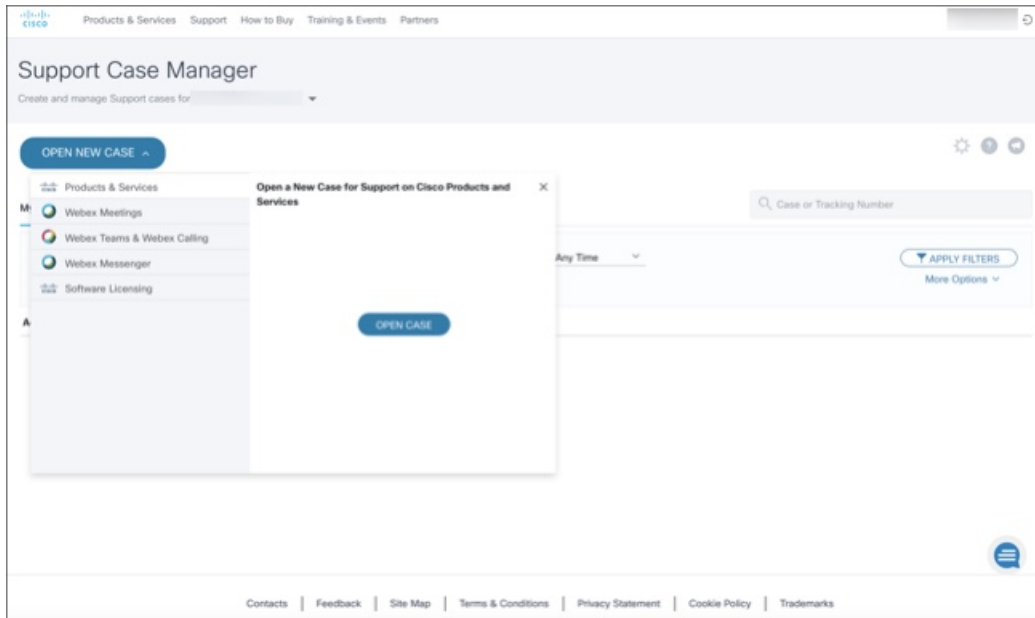
サポート

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> でサポートケースをオープンしてください。

手順

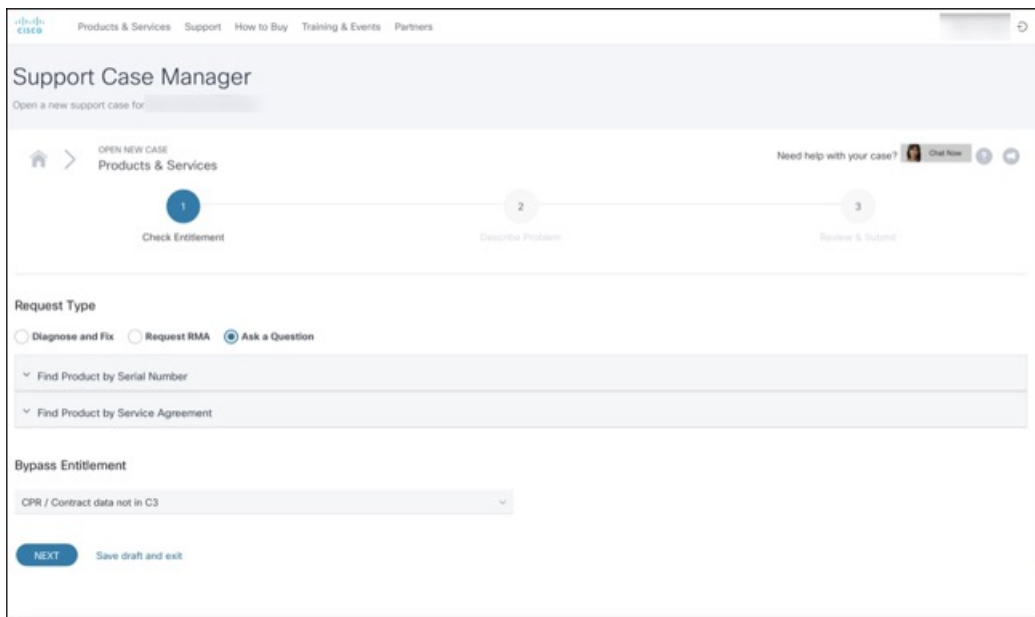
ステップ 1 Support Case Manager で、**[Open New Case]** > **[Open Case]** をクリックします。

図 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。

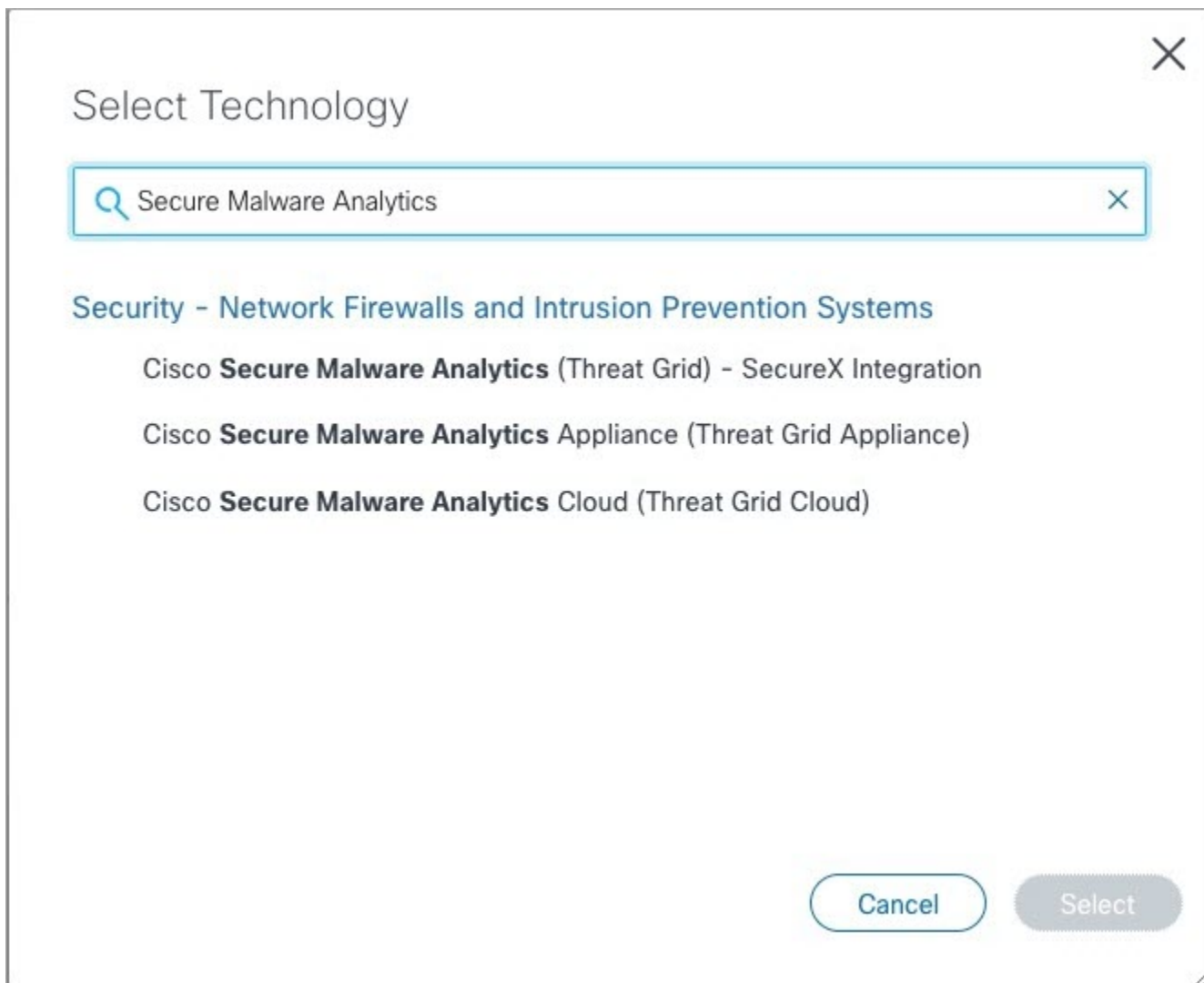
図 2:エンタイトルメントのチェック



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)] を入力します (タイトルで Cisco Secure Malware Analytics に言及してください)。

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 3: 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。

- 『*Cisco Secure Malware Analytics Appliance Administration Guide*』の「サポートモードとサポートスナップショットの有効化」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。

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
- 管理 UI 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



(注) 設定を完了するには、約 1 時間かかります。

管理者の設定が必要な追加のタスク（ライセンスのインストール、電子メールサーバー、SSL 証明書など）については、『*Cisco Secure Malware Analytics Appliance Administration Guide*』に記載されています。



第 2 章

初期ネットワーク設定

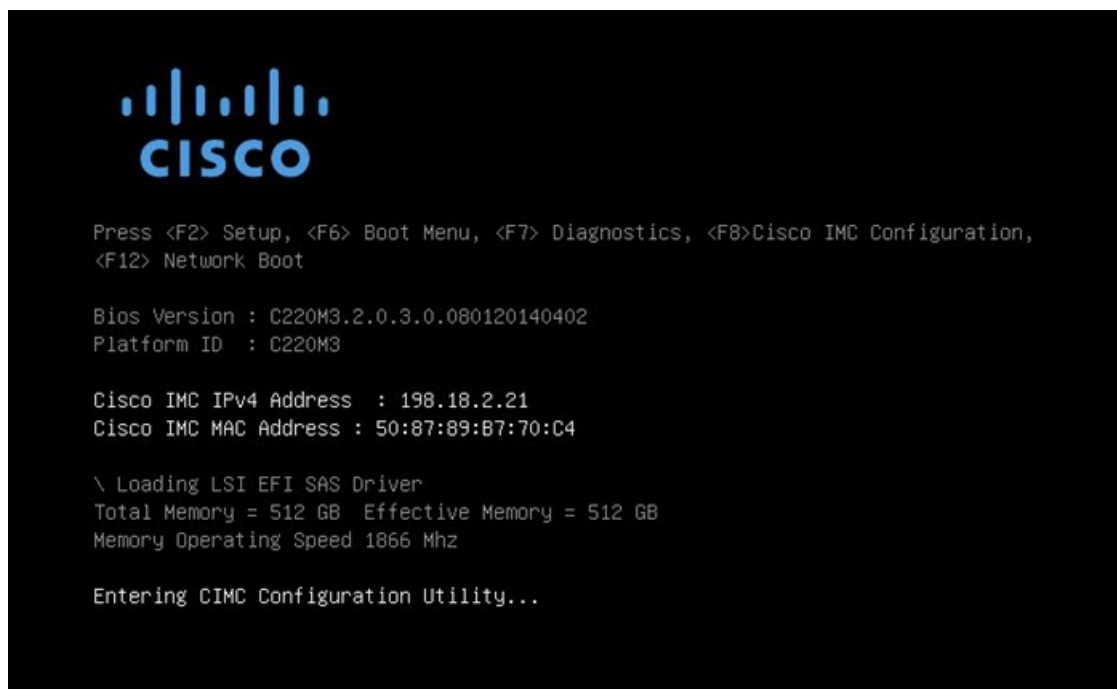
この章では、管理 TUI（テキストモード UI）を使用して初期ネットワーク設定を完了する手順について説明します。説明する項目は次のとおりです。

- [アプライアンスの電源オンと起動（9 ページ）](#)
- [管理 TUI を使用したネットワークの設定（10 ページ）](#)

アプライアンスの電源オンと起動

サーバーの周辺機器、ネットワーク インターフェイス、および電源ケーブルを接続したら、Secure Malware Analytics 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 4: ブートアップ時のシスコ画面



サーバー起動と接続が正常に終了すると、コンソールに [管理TUI (Admin TUI)] が表示されます。

図 5: 管理 TUI

```

Cisco Secure Malware Analytics - Appliance Administration
Your Malware Analytics appliance can be managed at:
Admin URL / MAC: https://10.90.3.100 / 3e:fd:fe:eb:f8:30
Application URL / MAC: https://10.90.2.100 / 5c:71:0d:26:00:46
Password: RNdLHmMc5hSG1tX764o
The password shown has been automatically generated for you.
You will be required to change this password when you first login.

(n) Network
    Configure the system's network interfaces
(r) Support Mode
    Allow remote access by customer support
(u) Updates
    Download and optionally install updates
(s) Snapshots
    Generate and submit snapshots
(a) Apply
    Apply configuration
(c) Console
    CLI-based configuration access
(e) Exit
    Exit the management tool
  
```

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管理 UI に到達できず、このタスクを実行できないため、[管理URL (Admin URL)] は利用不可として示されています。



重要 [管理TUI (Admin TUI)]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管理 UI にアクセスし、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。

管理 TUI 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、管理 TUI で完了します。基本設定が完了すると、管理 UI 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 ユーザーの場合、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せん。DHCP を使用して IP を取得している場合は、『[Cisco Secure Malware Analytics Appliance Administration Guide](#)』を参照してください。

手順

- ステップ 1** 管理 TUI で、[ネットワーク (Network)] を選択します。[ステータス : 設定 (Status: configuration)] 設定画面が表示されます。

図 6: 管理 TUI : ネットワーク設定コンソール

```
Cisco Secure Malware Analytics - Appliance Administration
Your Malware Analytics appliance can be managed at:
Admin URL / MAC: https://10.90.3.104 / 40:a6:b7:36:ed:e8
Application URL / MAC: https://10.90.2.104 / a4:88:73:58:43:0e
Password: *** set by user ***

Status: configuration current

(c) Clean
    Configure CLEAN interface
(d) Dirty
    Configure DIRTY interface
(a) Admin
    Configure ADMIN interface
(x) Activate
    Activate Network Configuration
(b) Back
    Go back
```

- ステップ 2** [クリーン (Clean)] を選択します。[ネットワーク設定 : クリーンインターフェイス (Network Config - CLEAN Interface)] 画面が表示されます。
- ステップ 3** ネットワーク管理者から提供された設定に従って、空白のフィールドに入力します。
- ステップ 4** [保存 (Save)] を選択します。
- ステップ 5** [ダーティ (Dirty)] を選択します。[ネットワーク設定 : ダーティインターフェイス (Network Config - Dirty Interface)] 画面が表示されます。

- ステップ 6** ネットワーク管理者から提供された設定に従って、空白のフィールドに入力します。
- ステップ 7** [保存 (Save)] を選択します。
- ステップ 8** [管理 (Admin)] を選択します。[ネットワーク設定 : 管理インターフェイス (Network Config - ADMIN Interface)] 画面が表示されます。
- ステップ 9** ネットワーク管理者から提供された設定に従って、空白のフィールドに入力します。
- ステップ 10** [保存 (Save)] を選択します。
- ステップ 11** [アクティブ化 (Activate)] を選択します。設定をアクティブにします。
-

次のタスク

Cisco Secure Malware Analytics アプライアンス設定の次の手順では、「[管理 UI の設定](#)」で説明されているように、管理 UI を使用して残りの設定タスクを完了します。



第 3 章

管理 UI の設定

この章では、管理 UI 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 \(13 ページ\)](#)
- [設定ウィザード \(16 ページ\)](#)
- [Cisco Secure Malware Analytics アプライアンスの更新をインストールする \(30 ページ\)](#)
- [アプライアンス設定のテスト \(31 ページ\)](#)

はじめに

Admin UI は、管理者が Cisco Secure Malware Analytics アプライアンスを設定するために使用する推奨ツールです。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 ユーザー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。

- 管理 UI の管理者パスワードの変更
- エンドユーザーライセンス契約書の確認
- ネットワークの設定
- ライセンスのインストール
- NFS の設定
- クラスタリングの設定
- 電子メールの設定
- 通知の設定
- 日付と時刻の設定
- システムログの設定
- 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 証明書やバックアップなど、ウィザードに含まれていない構成設定については、『[Cisco Secure Malware Analytics Appliance Administration Guide](#)』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。

管理 UI へのログイン

Cisco Secure Malware Analytics 管理 UI にログインするには、次の手順を実行します。

手順

ステップ 1 ブラウザで、管理 UI の URL (<https://<adminIP>/> または <https://<adminHostname>/>) を入力して、Cisco Secure Malware Analytics 管理 UI 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。

図 7: 管理 UI ログイン画面



ステップ 2 管理 TUI からコピーした初期設定の [管理パスワード (Admin Password)] を入力して、[ログイン (Log In)] をクリックします。

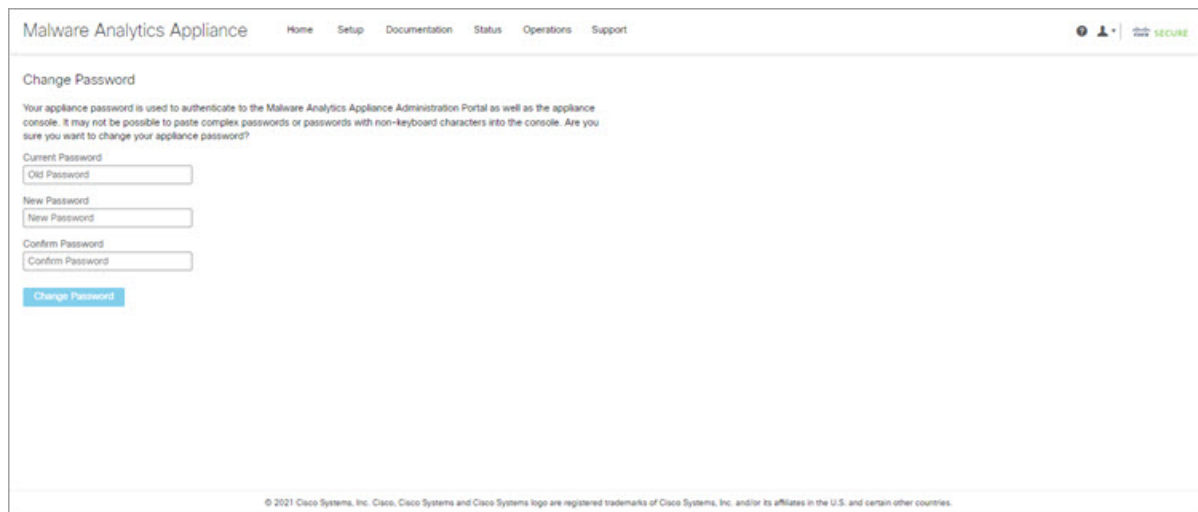
次のタスク

[Change Admin Password] [管理者パスワードの変更 \(15 ページ\)](#) 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 Cisco Secure Malware Analytics のインストール中にランダムに生成され、管理 TUI 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。

図 8: 管理者パスワードの変更



The screenshot shows the 'Change Password' interface in the Malware Analytics Appliance management console. At the top, there is a navigation bar with links for Home, Setup, Documentation, Status, Operations, and Support. The main heading is 'Change Password'. Below the heading is a warning message: 'Your appliance password is used to authenticate to the Malware Analytics Appliance Administration Portal as well as the appliance console. It may not be possible to paste complex passwords or passwords with non-keyboard characters into the console. Are you sure you want to change your appliance password?'. There are three input fields: 'Current Password' (with 'Old Password' label), 'New Password' (with 'New Password' label), and 'Confirm Password' (with 'Confirm Password' label). A blue 'Change Password' button is located below the input fields. At the bottom of the page, there is a small copyright notice: '© 2021 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.'

手順

- ステップ 1** 管理 TUI から取得した古いパスワードを [現在のパスワード (Current 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。
新しいパスワードには、最小 8 文字、1 つの数字、1 つの特殊文字、少なくとも 1 つの大文字と 1 つの小文字を含める必要があります。
- 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管理 TUI 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] [エンドユーザーライセンス契約書の確認 \(16 ページ\)](#) に進みます。

エンドユーザー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。

手順

ステップ 1 エンドユーザー 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 \(17 ページ\)](#) に進みます。

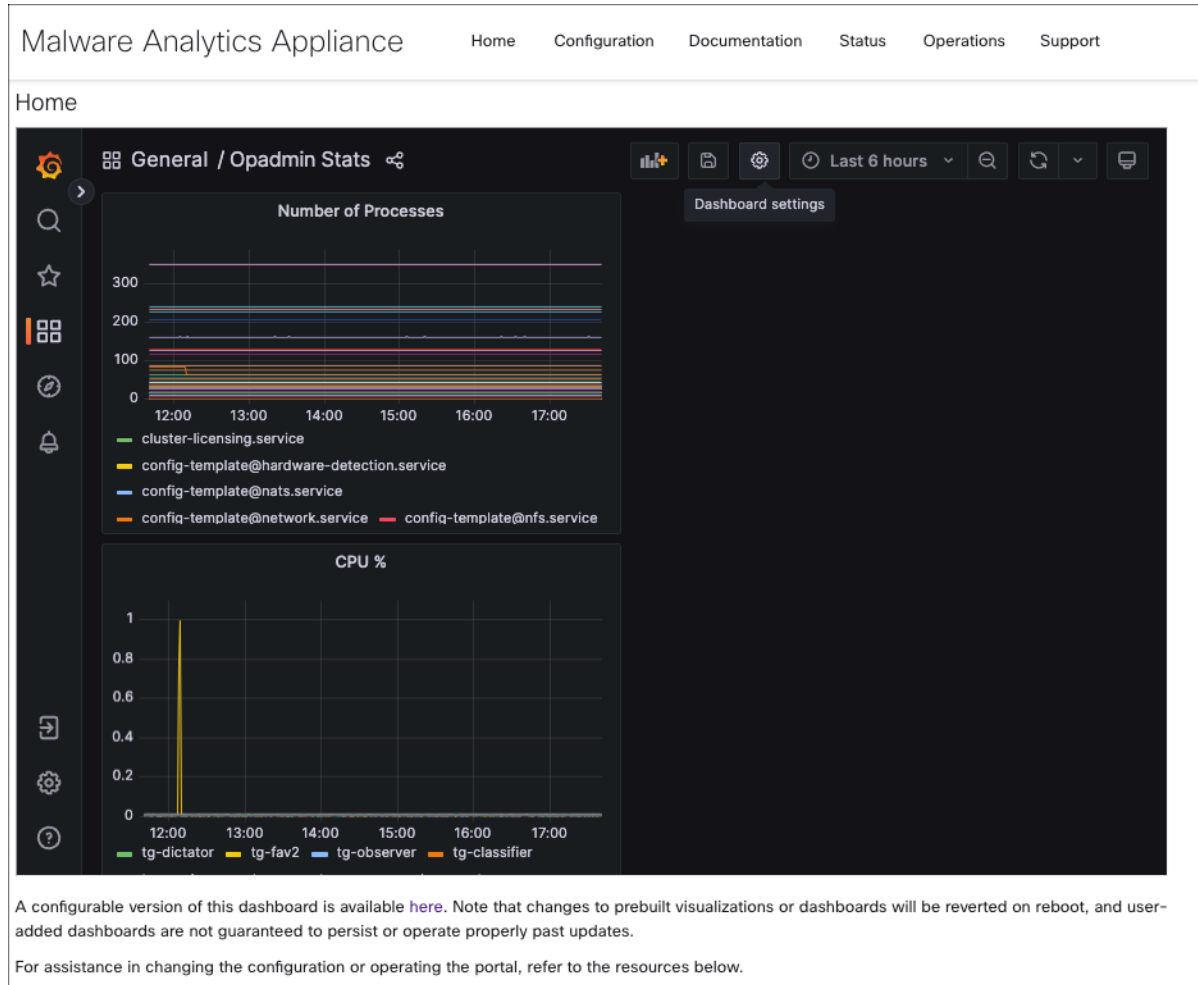
設定ウィザード

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

ウィザード設定の完了後に変更を加える必要がある場合は、管理 UI の [設定 (Configure)] タブから設定にアクセスできます。

Home

図 9: Home



ネットワークの設定

管理 TUI でスタティックネットワーク設定を行った場合、[ネットワーク設定 (Network Configuration)] ページに表示される IP アドレスは、Cisco Secure Malware Analytics ネットワーク設定中に管理 TUI に入力した値を反映します。

図 10: ネットワーク構成

The screenshot shows the Malware Analytics Appliance configuration wizard. The left sidebar lists the following steps: 1. Network (selected), 2. NFS, 3. Clustering, 4. License, 5. Email, 6. Notifications, 7. Date and Time, 8. System Log, and 9. Review and Install. The main content area is titled 'Network Configuration' and shows the 'CLEAN interface' configuration. The MAC Address is 'a4:88:73:58:43:0e' and the IP Address is '10.90.2.104 (DHCP)'. The IP Assignment is set to 'STATIC'. The IP Address field is empty. The Subnet Mask and Gateway fields are also empty. The Host Name is 'WMP243300XJ'. The Primary DNS Server and Secondary DNS Server fields are empty.

手順

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、『[Cisco Secure Malware Analytics Appliance Administration Guide](#)』の「DHCP の使用」の項の手順を実行します。

次のタスク

[NFS の設定 \(18 ページ\)](#) 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 Secure Malware Analytics Appliance Administration Guide](#)』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 Cisco Secure Malware Analytics 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。

この手順をスキップするか、続行して後で戻る場合は、[NFS なしで続行 (Continue without NFS)] をクリックします。

手順

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設定 (NFS Configuration)] ページを開きます。

ステップ 2 次の情報を入力します。クラスタ内のアプライアンスは、最初のクラスタノードで設定されているものと同じホストとパスを共有する必要があります。

- **[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。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。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。)

ステータスは **Enabled_Pending** キーです。

ステップ 3 [保存 (Save)] をクリックします。ページが更新されます。[生成 (Generate)] 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。

(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。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。

ステップ 4 [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 5 [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。[アップロード (Upload)] ボタンが [ダウンロード (Download)] ボタンに変わります。

ステップ 6 [ダウンロード (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。

このアプライアンスがクラスタ内の最初のノードである場合、追加のノードをクラスタに結合させるためのキーが必要になります。最初のノードがすでに設定されている場合は、[アップロード (Upload)] をクリックし、新しいクラスタを開始したときに最初のノードからダウンロードした NFS 暗号化キーを選択します。

ステップ 7 [保存 (Save)] をクリックします。

ページが更新されます。[キーID (Key ID)] が表示され、[アクティブ化 (Activate)] ボタンが有効になります。

ステップ 8 [アクティブ化 (Activate)] をクリックします。

数秒後に [Status] が [Active] に変わります (左下隅)。

ステップ 9 アクティベーションが成功したら、[続行 (Continue)] をクリックします。

次のタスク

[クラスタリングの設定 (Configure Clustering)] [最初のクラスタノードの設定 \(21 ページ\)](#) に進みます。

クラスタリングの設定

ウィザードワークフローの次のステップは、クラスタリングの設定です。設定中のアプライアンスがクラスタの一部にならない場合は、次の設定手順、[ライセンスのインストール \(22 ページ\)](#) へ進みます。

クラスタリングの主な目的は、単一システムのサンプル分析能力を高めることです。クラスタ内の各アプライアンスは、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。クラスタリングによってストレージ容量は増加せず、サンプル分析の速度も向上しません。代わりに、クラスタリングを使用すると、単一のアプライアンスで達成できるのと同じ時間で、より多くのサンプルを分析できます。データはすべてのノードで同じであるため、サンプル分析を送信ノードから、それほどビジーではない別のクラスタノードに渡すことができます。クラスタには、2~7台のアプライアンスを含めることができます。

さらにクラスタリングは、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。

新しいアプライアンス、データが削除された (ワイプされていない) アプライアンス、または新規および既存のアプライアンスの組み合わせでクラスタを作成できます。Cisco Secure Malware Analytics アプライアンスをクラスタに結合する場合、初期設定時に NFS とクラスタリングが設定されていると便利です。[クラスタ設定 (Cluster Configuration)] ページからインストール後のクラスタを開始できますが、インストール済みのアプライアンスを既存のクラスタに結合させることはできません。

クラスタリングの詳細については、『[Secure Malware Analytics Appliance Administrator Guide v2.17](#)』を参照してください。

クラスタのインストールまたは再設定について質問がある場合は、[サポート (Support)] [サポート \(4 ページ\)](#) にお問い合わせください。



(注) 既存のアプライアンスをクラスタに結合させる場合は、『[Secure Malware Analytics Appliance Administrator Guide v2.17](#)』の「アプライアンスをバックアップまたは復元対象としてリセット」セクションに記載されているように、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。

最初のクラスタノードの設定

最初のノードを設定してクラスタを開始し、追加の各ノードを設定し、最初のノードの設定時にダウンロードした NFS キーを使用してそれらをクラスタに結合させます。

最初のノードを既に設定している場合は、[追加のクラスタノードへの結合 (Joining Additional Cluster Nodes)] [追加のクラスタノードへの結合 \(21 ページ\)](#) に進みます。

クラスタは、[クラスタ設定 (Cluster Configuration)] ページの管理 UI で設定および管理されます。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)。

手順

-
- ステップ 1** ナビゲーションペインで [クラスタリング (Clustering)] をクリックして、[クラスタ設定 (Cluster Configuration)] ページを開きます。
 - ステップ 2** [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 3** 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 4** [クラスタリング (Clustering)] ページで、新しいクラスタの状態を確認します。
-

次のタスク

[追加のクラスタノードへの結合 (Joining Additional Cluster Nodes)] [追加のクラスタノードへの結合 \(21 ページ\)](#) に進みます。

追加のクラスタノードへの結合

このセクションでは、追加のアプライアンスをクラスタに結合させる方法について説明します。クラスタ内の最初のアプライアンスが、「[最初のクラスタノードの設定](#)」で説明されているように設定されていることを前提としています。これで、次のノードの設定手順を開始できます。

手順

-
- ステップ 1** [設定 (Configuration)] タブをクリックし、[NFS] を選択して [NFS設定 (NFS Configuration)] ページを開きます。
 - ステップ 2** クラスタ内の最初のノードで設定されたものと一致するように、[ホスト (Host)] と [パス (Path)] を指定します。

- ステップ 3** [保存 (Save)] をクリックします。ページが更新され、[アップロード (Upload)] ボタンが使用可能になります。
- ステップ 4** [設定 (Configuration)] メニューで、[クラスタリング (Clustering)] を選択して [クラスタの設定 (Cluster Configuration)] ページを開きます。
- ステップ 5** [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。
[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 6** インストールを終了します。これにより、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 7** クラスタに結合させるノードごとに手順を繰り返します。

次のタスク

[ライセンスのインストール \(22 ページ\)](#) に進みます。

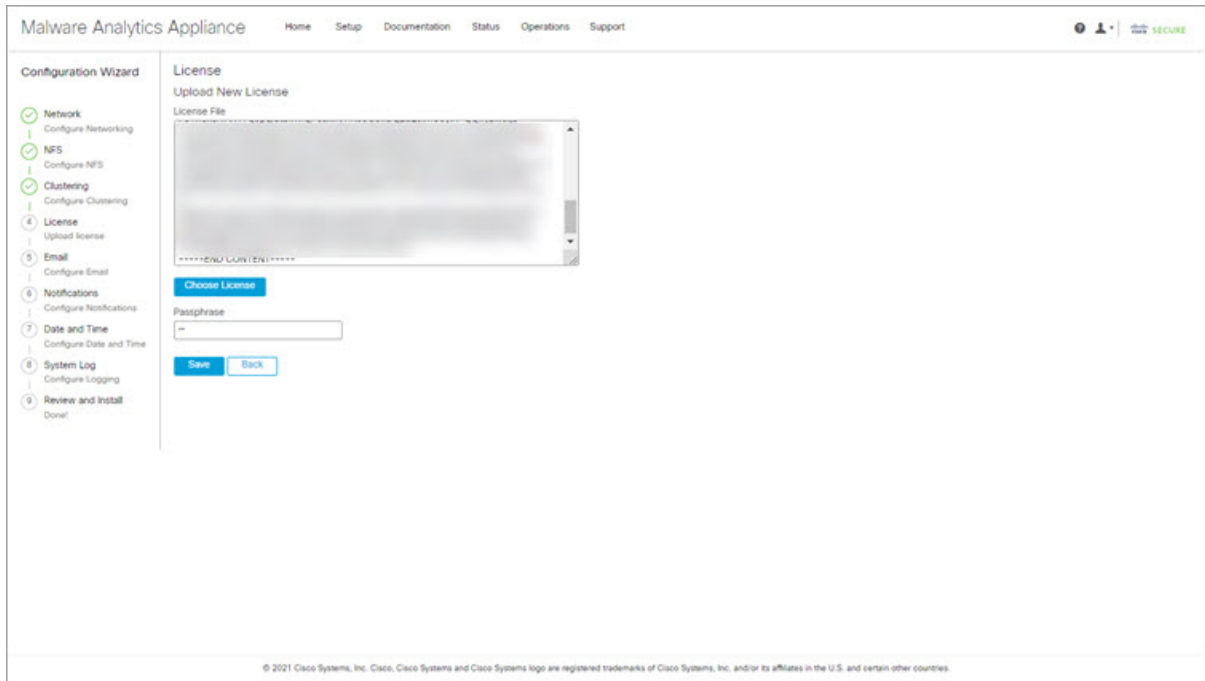
ライセンスのインストール

クラスタリングが完了すると、Cisco Secure Malware Analytics ライセンスをインストールする準備が整います。

手順

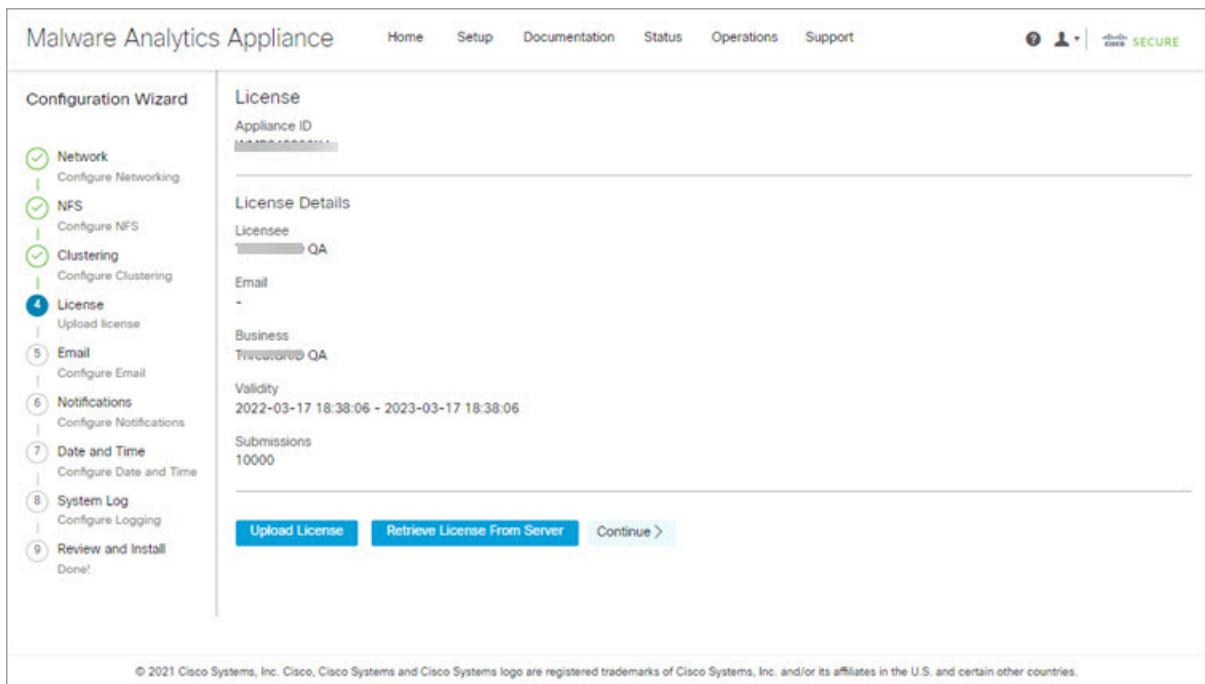
- ステップ 1** [ライセンスのアップロード (Upload License)] をクリックし、ファイルマネージャからライセンスファイルを選択します。
- または、サーバーからライセンスを取得することもできます。アプライアンスを設置した時点ネットワークにアクセス可能な場合は、[サーバーからライセンスを取得 (Retrieve License From Server)] をクリックするとライセンスがネットワーク経由で取得されます。
- ステップ 2** [Passphrase] フィールドにライセンスのパスワードを入力します。

図 11: 新規ライセンスのアップロード



ステップ 3 [保存 (Save)] 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 12: インストールが成功した後のライセンス情報



ステップ 4 [続行 (Continue)] をクリックします。

次のタスク

電子メールの設定 (24 ページ) に進みます。

電子メールの設定

ワークフローの次の手順は、[SMTP設定 (SMTP Configuration)] ページの電子メールホストを設定することです。

手順

ステップ 1 [送信元電子 (From Address)] メールアドレスを入力します。

図 13: SMTP の設定

The screenshot shows the Malware Analytics Appliance configuration wizard. On the left, a 'Configuration Wizard' sidebar lists steps: Network, NFS, Clustering, License, Email (selected), Notifications, Date and Time, System Log, and Review and Install. The main area is titled 'SMTP Configuration' and contains the following fields:

- From Address: [Empty text input field]
- Upstream Host: [host name]
- Upstream Port: [587]
- Encryption: [None]
- Upstream Authentication: [None]

At the bottom of the configuration area, there are three buttons: 'Save', 'Send Test Email', and 'Continue >'. The footer of the page reads: '© 2021 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.'

ステップ 2 [アップストリームホスト (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 [保存 (Save)] をクリックして設定を保存します。

ステップ 6 [続行 (Continue)] をクリックして、ワークフローの次のステップに進みます。

次のタスク

[Configure Notifications]通知の設定 (25 ページ) に進みます。

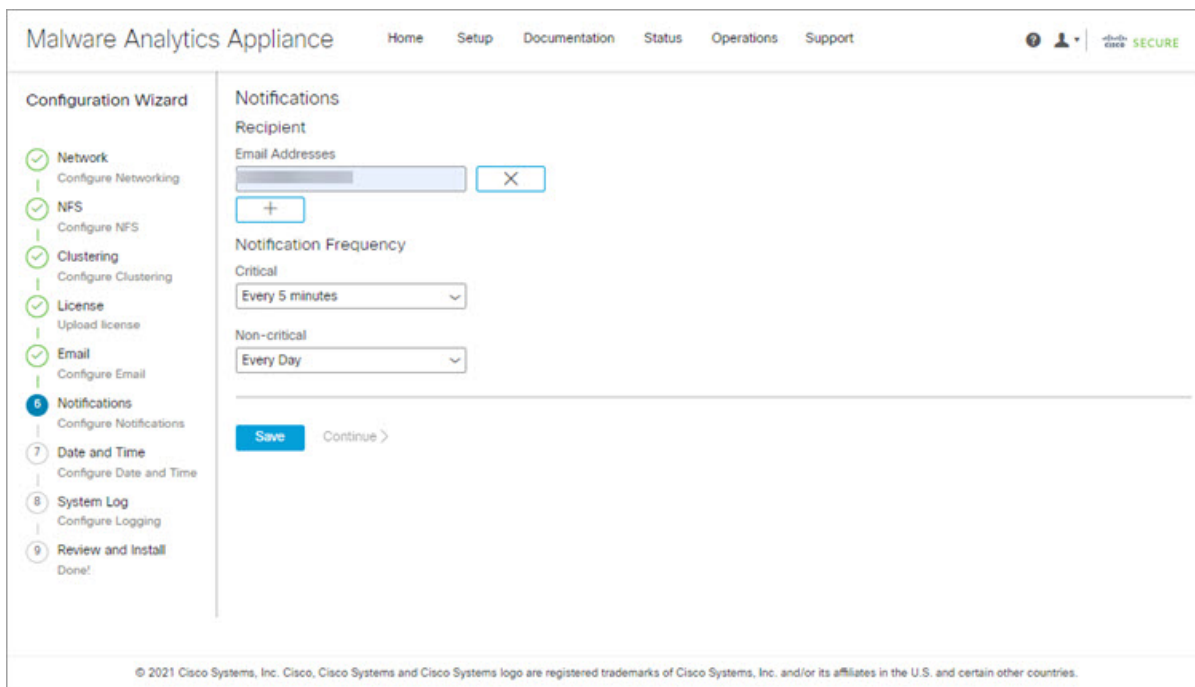
通知の設定

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 Cisco Secure Malware Analytics ポータルインターフェイスに表示されますが、このページで、電子メールで送信される [通知 (Notifications)] も設定できます。

手順

ステップ 1 [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。

図 14: Notifications



The screenshot shows the Malware Analytics Appliance configuration wizard. The left sidebar lists the steps: Network, NFS, Clustering, License, Email, Notifications (current step), Date and Time, System Log, and Review and Install. The main content area is titled 'Notifications' and includes a 'Recipient' section with an 'Email Addresses' input field and a '+ ' button. Below that is the 'Notification Frequency' section with two dropdown menus: 'Critical' (set to 'Every 5 minutes') and 'Non-critical' (set to 'Every Day'). At the bottom of the main area are 'Save' and 'Continue >' buttons. The footer contains copyright information for Cisco Systems, Inc. © 2021.

ステップ 2 [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 3 [保存 (Save)] をクリックします。

ステップ 4 [続行 (Continue)] をクリックして、ワークフローの次のステップに進みます。

次のタスク

[日付と時刻の設定 (Configure Date and Time)] [日付と時刻の設定 \(26 ページ\)](#) に進みます。

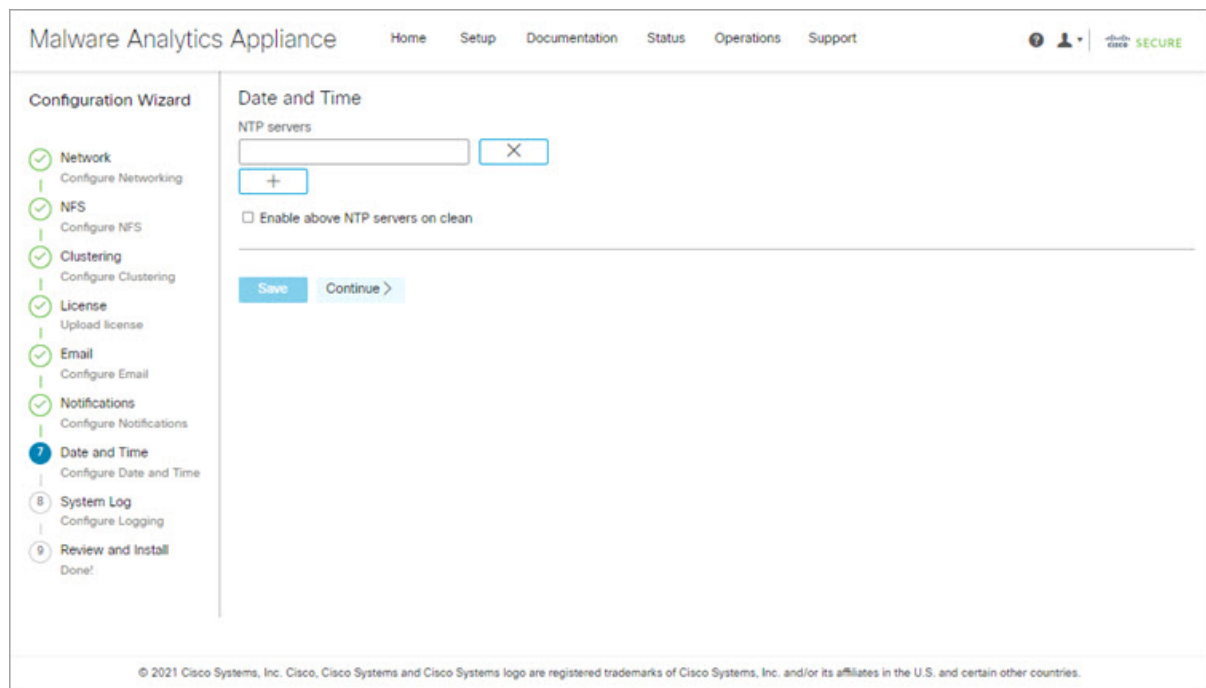
日付と時刻の設定

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

手順

ステップ 1 [NTP Server(s)] に、NTP サーバーの IP または NTP 名を入力します。

図 15: 日付および時刻 (*Date and Time*)



複数の NTP サーバーがある場合は、[+] 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 2 [保存 (Save)] をクリックします。

ステップ 3 [続行 (Continue)] をクリックして、ワークフローの次のステップに進みます。

次のタスク

[システムログの設定 (Configure System Log)] [システムログの設定 \(27 ページ\)](#) に進みます。

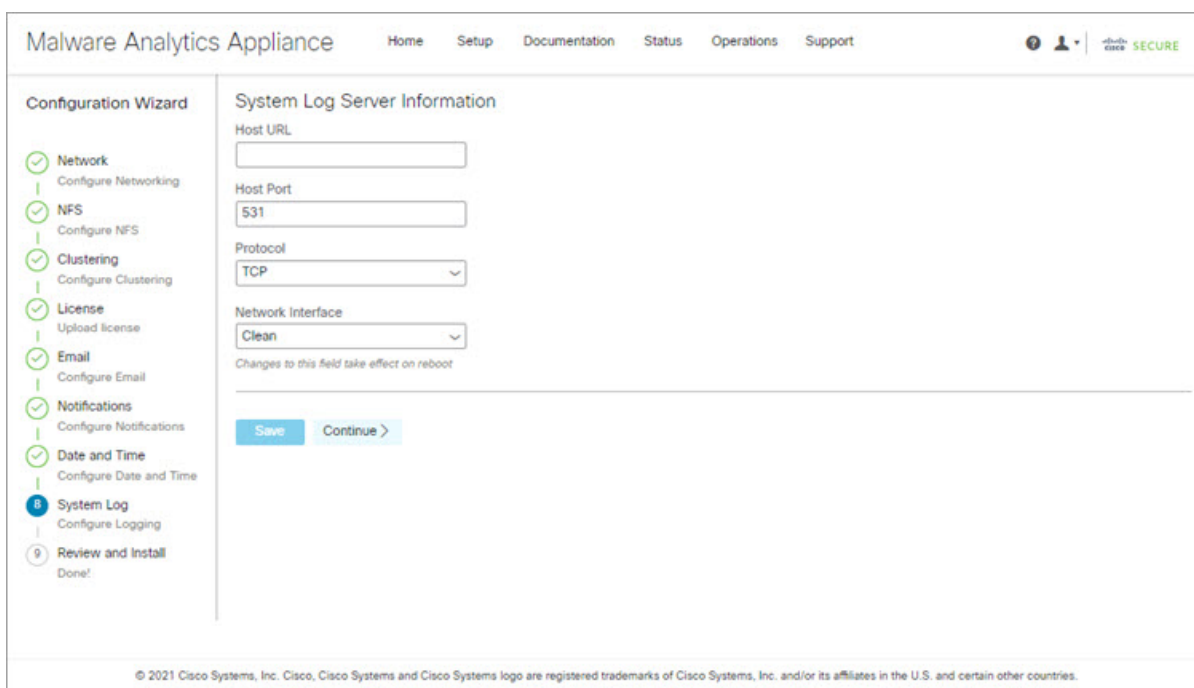
システムログの設定

[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 [ホスト URL (Host URL)]、[ホストポート (Host Port)]、および [プロトコル (Protocol)] フィールドに入力し、[保存 (Save)] をクリックします。

図 16: システムログサーバー情報



The screenshot shows the Malware Analytics Appliance configuration interface. The page title is "Malware Analytics Appliance" with navigation links for Home, Setup, Documentation, Status, Operations, and Support. A "Configuration Wizard" sidebar on the left lists steps: Network, NFS, Clustering, License, Email, Notifications, Date and Time, System Log (highlighted with a blue circle and '8'), and Review and Install (highlighted with a grey circle and '9'). The main content area is titled "System Log Server Information" and contains the following fields: Host URL (text input), Host Port (text input with value "531"), Protocol (dropdown menu with "TCP" selected), and Network Interface (dropdown menu with "Clean" selected). Below the fields is a note: "Changes to this field take effect on reboot". At the bottom of the form are "Save" and "Continue >" buttons. A copyright notice at the bottom reads: "© 2021 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries."

ステップ 2 [続行 (Continue)] をクリックして、ワークフローの最後のステップに進みます。

詳細については、『[Cisco Threat Grid Appliance Administration Guide](#)』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 \(27 ページ\)](#) に進みます。

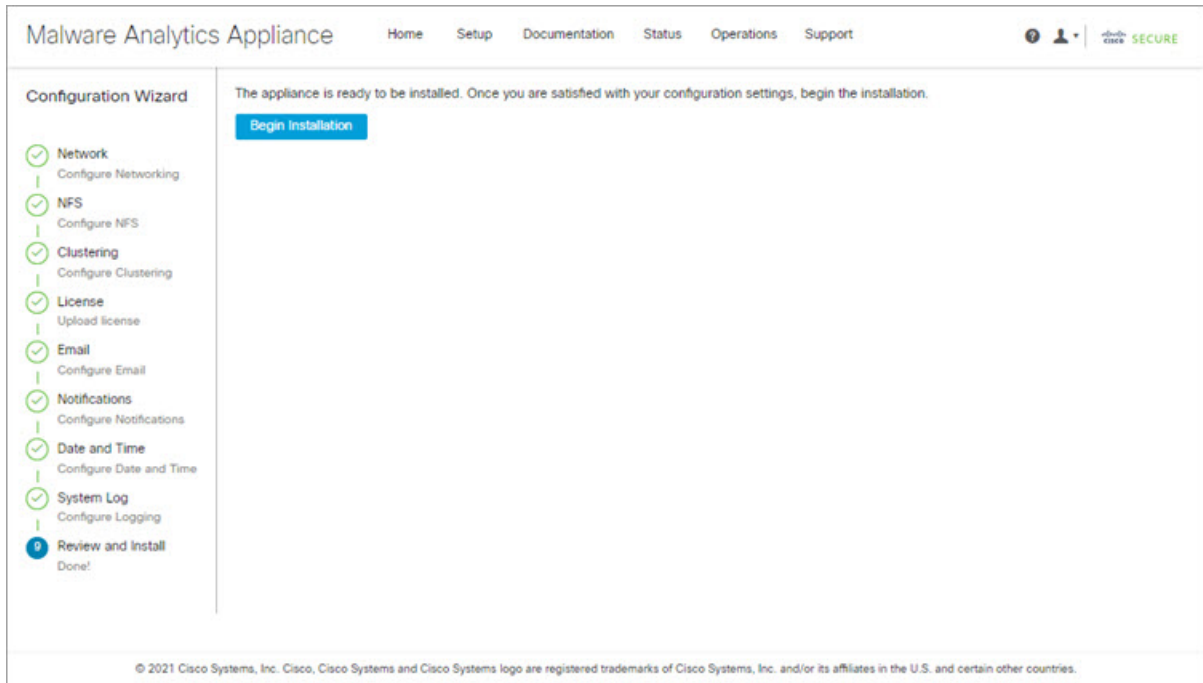
設定の確認とインストール

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。

手順

ステップ 1 ナビゲーションペインで[レビューおよびインストール (Review And Install)] をクリックし、次に[インストールの開始 (Begin 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。

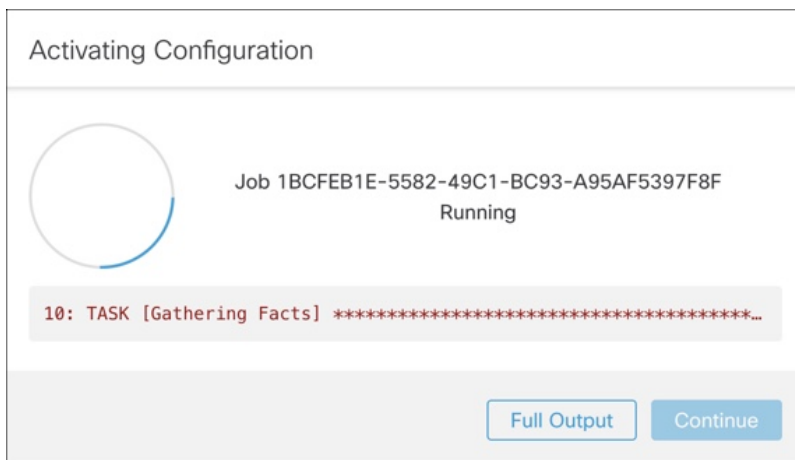
図 17: インストールの開始



(注)

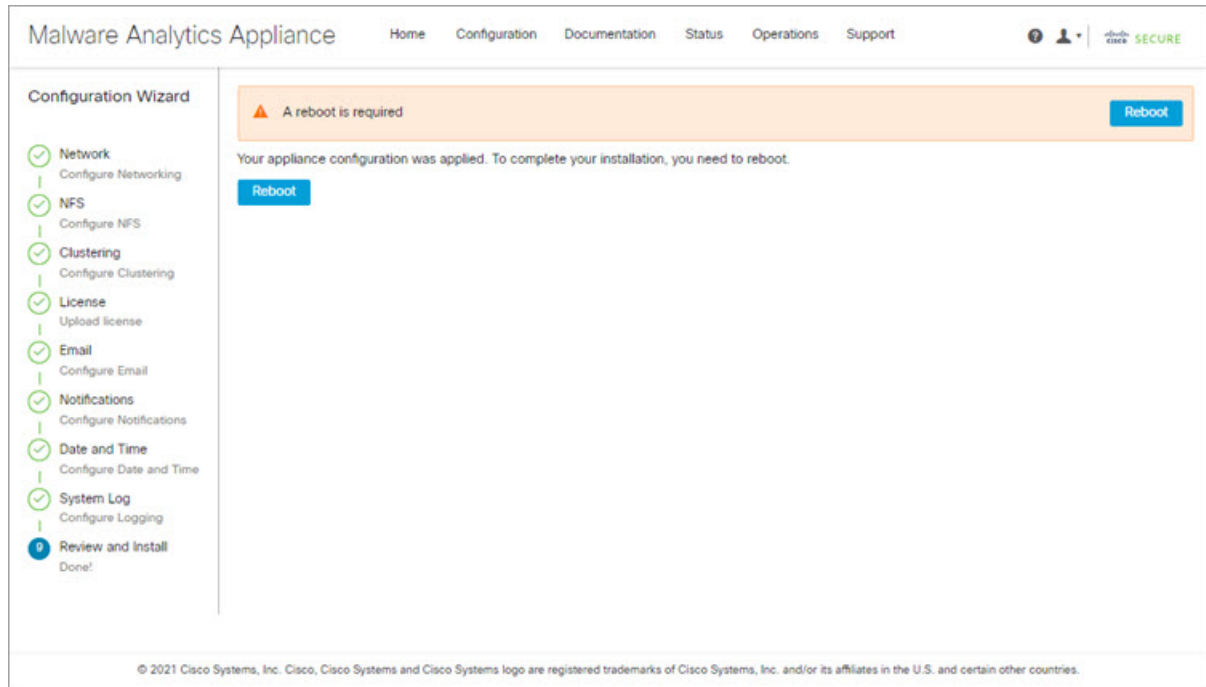
この画面には、設定の適用状況に応じて設定情報が表示されます。

図 18: 設定のアクティブ化



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 19: アプライアンスのインストール成功

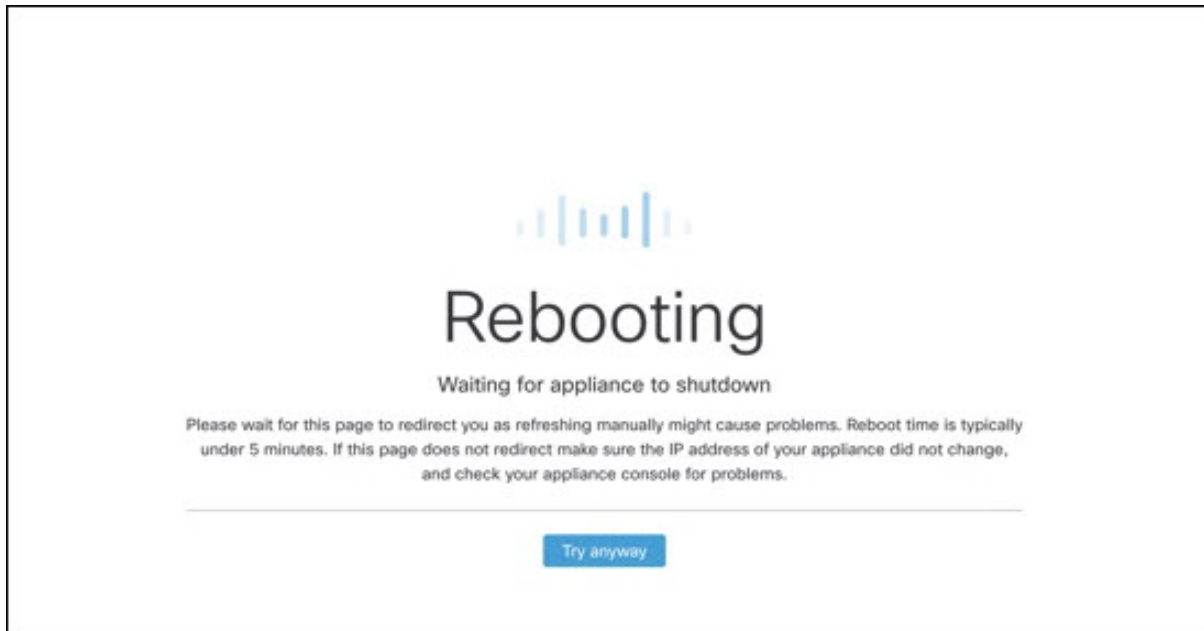


ステップ 2 [Reboot] をクリックします。

(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 20: アプライアンスは再起動中です



再起動後、アプライアンスは管理 UI [ホーム (Home)] ページを開きます。これで設定プロセスは完了です。

Cisco Secure Malware Analytics アプライアンスの更新をインストールする

初期 Cisco Secure Malware Analytics アプライアンスの設定後は、続行前に、利用可能な商品をインストールすることをお勧めします。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。

エアギャップ実装を使用しているユーザーは、[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。

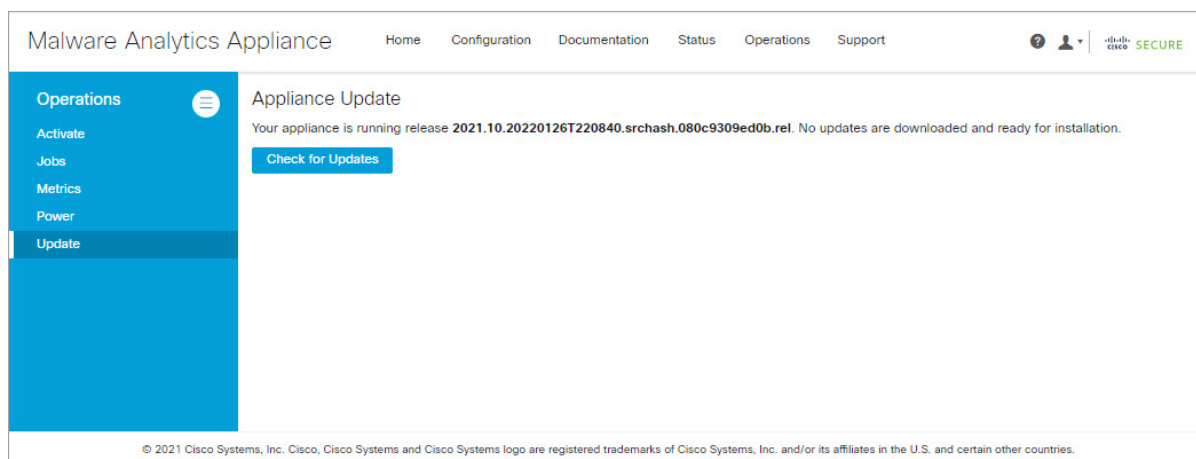


(注) 更新のインストールの詳細については、『[Cisco Secure Malware Analytics Appliance Administration Guide](#)』を参照してください。

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 21: 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。

アプライアンス設定のテスト

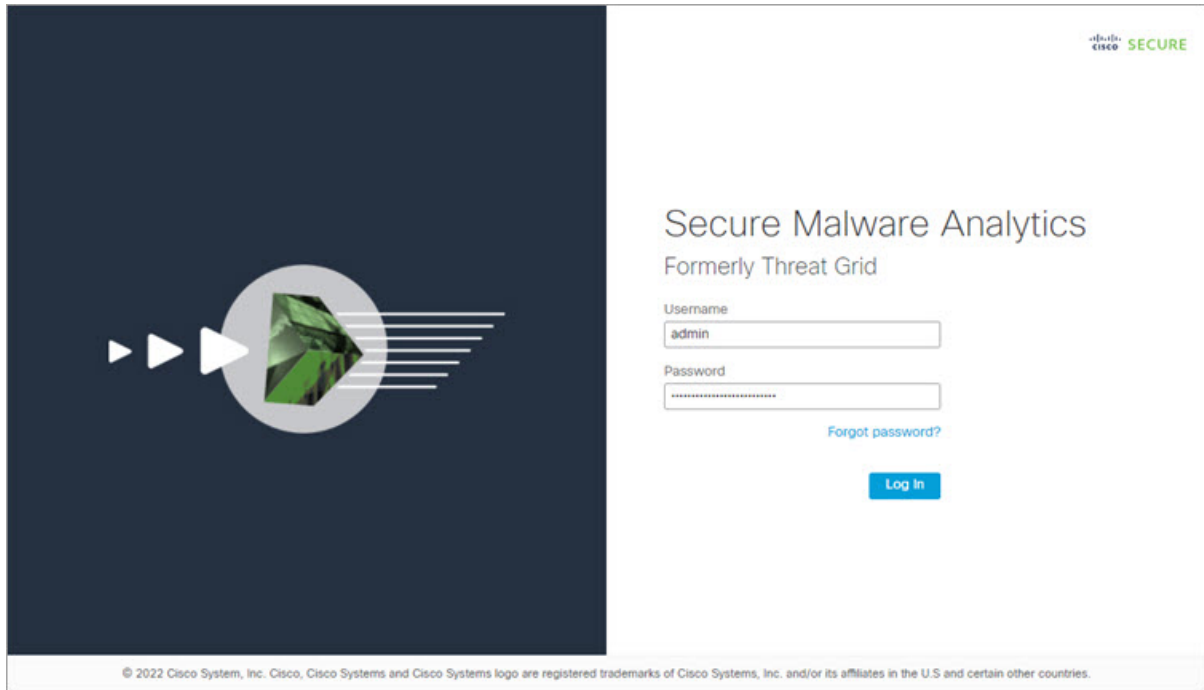
Cisco Secure Malware Analytics を使用アプライアンスが現行のバージョンに更新されたら、Cisco Secure Malware Analytics にマルウェアサンプルを送信して、アプライアンスが正しく設定されていることをテストする必要があります。

手順

ステップ 1 ブラウザで、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、Cisco Secure Malware Analytics を開きます。

Cisco Secure Malware Analytics ログインページが開きます。

図 22: Cisco Secure Malware Analytics ログイン

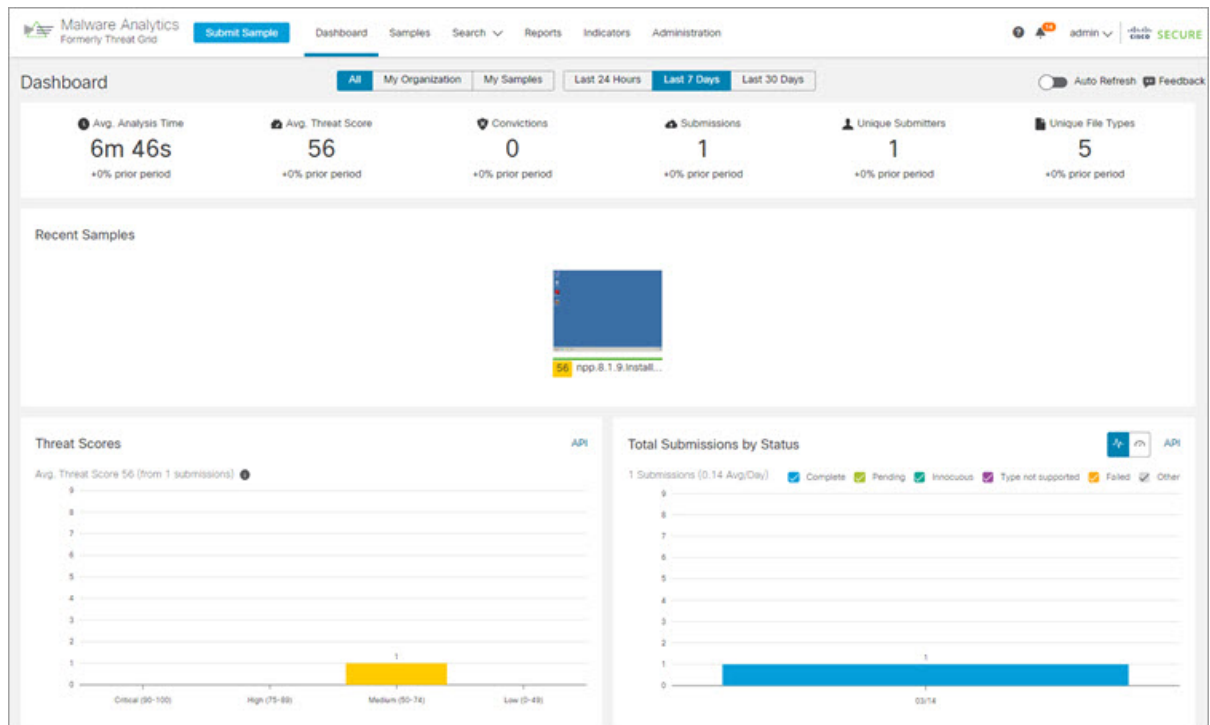


ステップ 2 次のデフォルトの資格情報を入力します。

- ログイン : **admin**
- パスワード : 管理 UI の設定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 [ログイン (Log In)] をクリックして、メインの [Cisco Secure Malware Analytics] ダッシュボードを開きます。サンプルデータはまだありません。

図 23: Cisco Secure Malware Analytics ダッシュボード



ステップ 4 [サンプルの送信 (Submit a Sample)] をクリックして、サンプルの送信ダイアログを開きます。

図 24: サンプルの送信

Submit Sample [X]

Submission Type: **Upload file** | Submit URL 🔍 Lookup

File: **Browse...** []

Options Templates ▾

Tags: []
zeus, spy-eye, etc...

Access: Mark private

Notification: Email me when analysis is complete

Virtual Machine ⓘ: [Use best option ▾]

Playbook: [None ▾]

[> Description]

Network Simulation ⓘ: **None** | As Needed | All Simulated
No network traffic will be simulated.

Network Exit ⓘ: [🌐 RMT - Unspecified - Remote ▾]

Callback URL: []
e.g. http://yourserver.com/callback/url, include http:// or https://

Runtime: [5 minutes ▾]

Password ⓘ: []

[> Sample Rules and Artifact Retention Policy]

[Create Options Template] [Cancel] [Submit]

(注)

このフォームの下部には、サンプルの送信ファイルの種類、サイズ、およびその他の情報を説明するヘルプがあります。[?]をクリックすることもできます。右上隅にあるアイコンをクリックすると、Cisco Secure Malware Analytics のリリースノートとオンラインヘルプが表示されます。これには、サンプルを送信して分析結果を確認する方法に関する完全なドキュメントが含まれます。

ステップ 5 ファイルをアップロードするか、マルウェア分析のために送信する URL を入力します。他のオプションの意味がわからない場合は、デフォルトのままにしてください。

ステップ 6 [送信 (Submit)] をクリックします。

Cisco Secure Malware Analytics サンプル分析プロセスが開始されます。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[サンプル (Samples)] ページに表示されます。分析が完了すると、分析レポートに結果が表示されます。

図 25: 分析レポート

The screenshot displays the 'Report' page for a sample named 'npp.8.1.9.installer.x64.exe'. The interface includes a navigation menu on the left with options like Metadata, Indicators, Network, TCP/IP Streams, Processes, Artifacts, and File Activity. The main content area is divided into 'Metadata' and 'Behavioral Indicators' sections.

Metadata

Sample ID	4a648f01929e772fe085d525d12a9ecb	Filename	npp.8.1.9.installer.x64.exe
Login	admin	Magic Type	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft installer self-extracting archive
Name	Administrator	File Type	exe
Access	Public	First Seen	3/14/22 9:19:23 am
OS	Windows 7 64-bit	Last Seen	3/14/22 9:19:23 am
Started	3/14/22 9:19:30 am	SHA-256	23bde004114ee4d17b11608da2c78fda365...
Ended	3/14/22 9:26:09 am	SHA-1	ca64fe1532504e1fddb01a829cbee70924ba58a
Duration	0:06:39	MDS	f58f00cbe75b26b1cfd112ad1537545
Sandbox	WMP243300XJ	Tags	
Playbook	No Playbook Applied		
Network Exit	LO - Local - Dirty Network Interface		
Localization			
Threat Score	56		

Behavioral Indicators

Title	Categories	ATT&CK	Tags	Hits	Score
Process Modified File in a User Directory	Dynamic Anomaly		executable, file, process	2	56
Static Analysis Flagged Artifact As Anomalous	Static Anomaly	Defense Evasion	anomaly, static	2	48
Memory Block Allocation with Read/Write/Execute Permissions	Code Injection	Defense Evasion, Privilege Escalation	memory	2	25
Artifact With Multiple Extensions Detected	Obfuscation	Defense Evasion	obfuscation	2	21
Executable Signed With Digital Certificate	Attribute		attributes, file	16	10

次のタスク

Cisco Secure Malware Analytics 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ー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 Secure Malware Analytics Appliance Administration Guide](#)』を参照してください。

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。