



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 \(1 ページ\)](#)
- [設定ウィザード \(4 ページ\)](#)
- [Cisco Secure Malware Analytics アプライアンスの更新をインストールする \(18 ページ\)](#)
- [アプライアンス設定のテスト \(19 ページ\)](#)

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 1: 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。

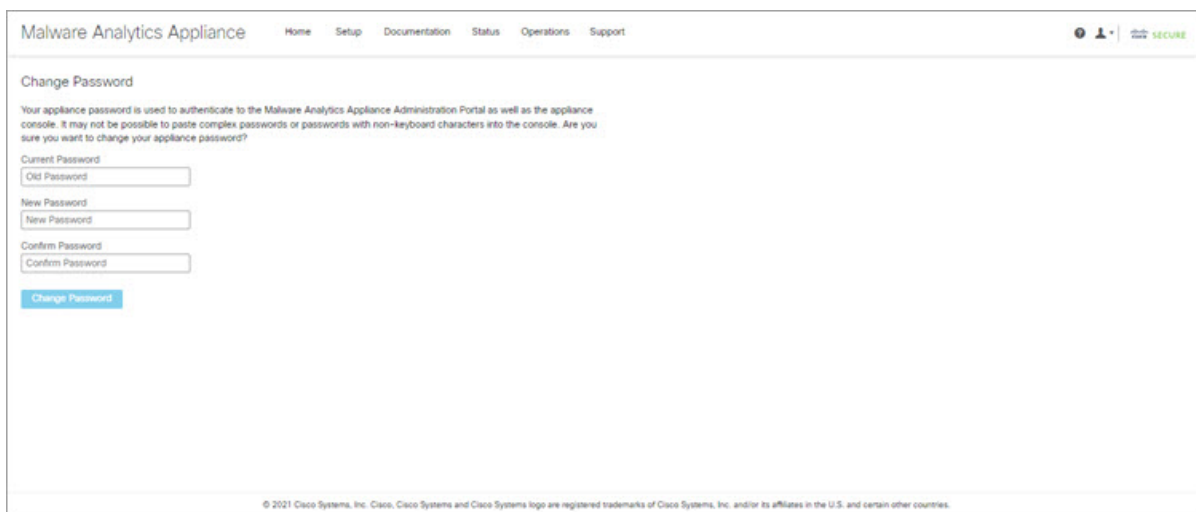
次のタスク

[Change Admin Password] [管理者パスワードの変更 \(3 ページ\)](#) 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 2: 管理者パスワードの変更



The screenshot shows the 'Change Password' page in the Malware Analytics Appliance management interface. The page has a navigation bar with links for Home, Setup, Documentation, Status, Operations, and Support. The main content area is titled 'Change Password' and contains 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?'. Below the warning are three input fields: 'Current Password' (with 'Old Password' placeholder), 'New Password' (with 'New Password' placeholder), and 'Confirm Password' (with 'Confirm Password' placeholder). 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 Agreemen][エンドユーザーライセンス契約書の確認 \(4 ページ\)](#)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 \(5 ページ\)](#)に進みます。

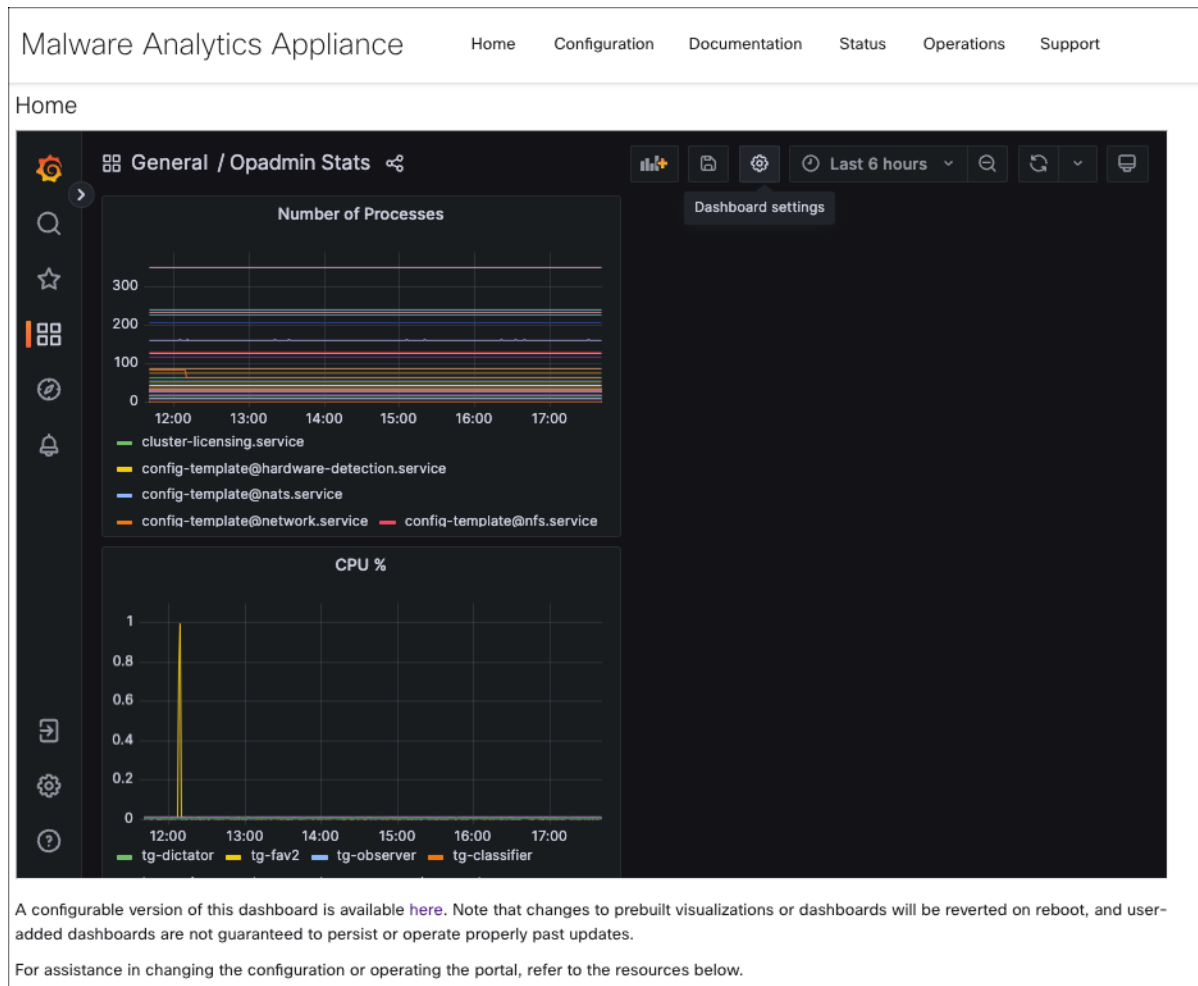
設定ウィザード

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 3: 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 4: 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'. There are input fields for IP Address, Subnet Mask, Gateway, Host Name (WMP243300XJ), Primary DNS Server, and Secondary DNS Server.

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 \(6 ページ\)](#) 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 \(9 ページ\)](#) 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 \(10 ページ\)](#) 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](#) 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 \(9 ページ\)](#) 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 \(9 ページ\)](#) 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 \(10 ページ\)](#) に進みます。

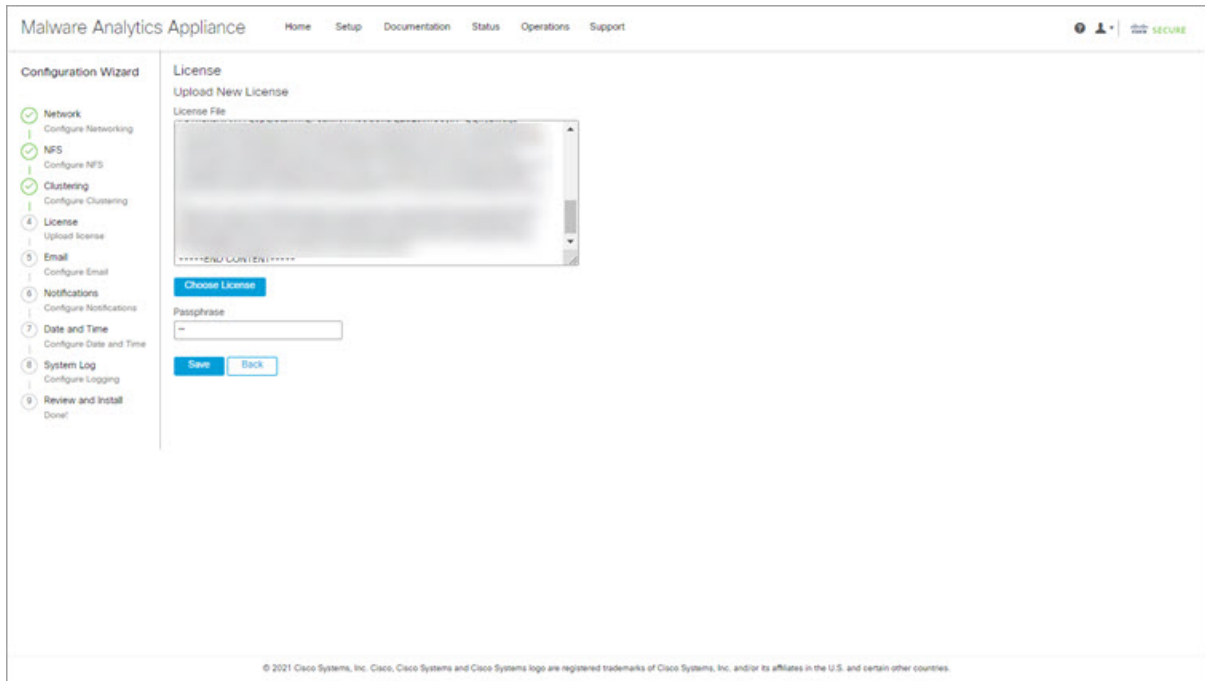
ライセンスのインストール

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

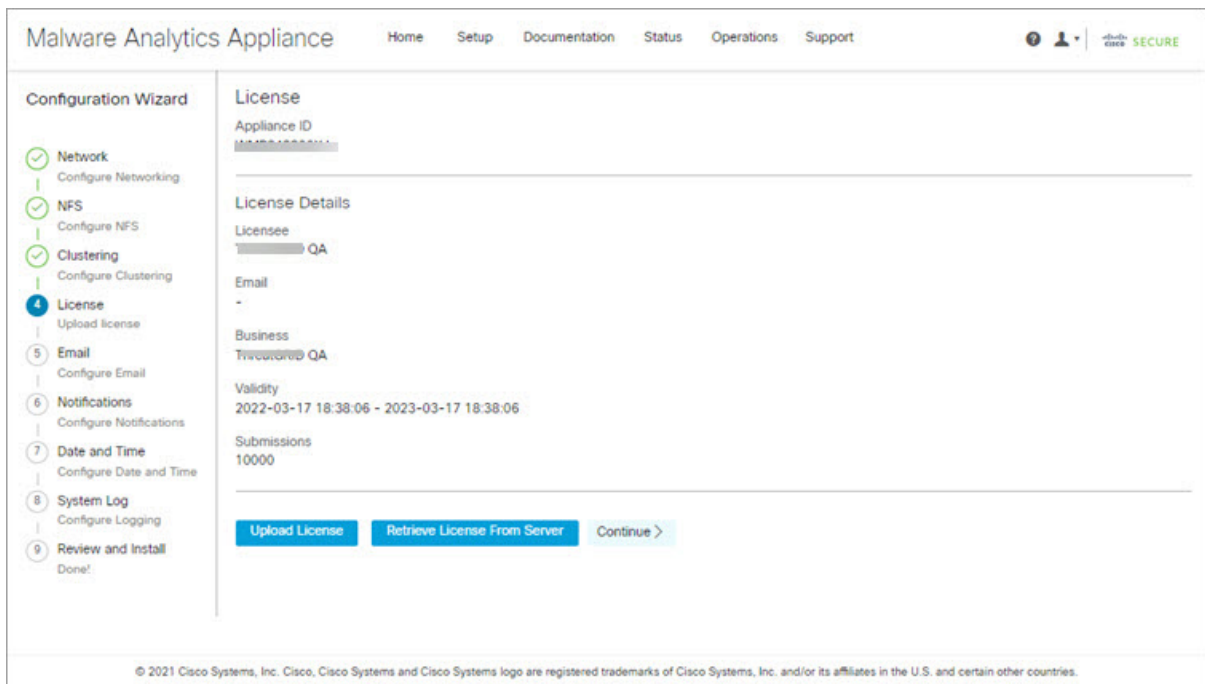
-
- ステップ1** [ライセンスのアップロード (Upload License)] をクリックし、ファイルマネージャからライセンスファイルを選択します。
- または、サーバーからライセンスを取得することもできます。アプライアンスを設置した時点ネットワークにアクセス可能な場合は、[サーバーからライセンスを取得 (Retrieve License From Server)] をクリックするとライセンスがネットワーク経由で取得されます。
- ステップ2** [Passphrase] フィールドにライセンスのパスワードを入力します。

図 5: 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 6: 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 (12 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 7: 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:
- Upstream Host:
- Upstream Port:
- Encryption:
- Upstream Authentication:

At the bottom of the form 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 (13 ページ) に進みます。

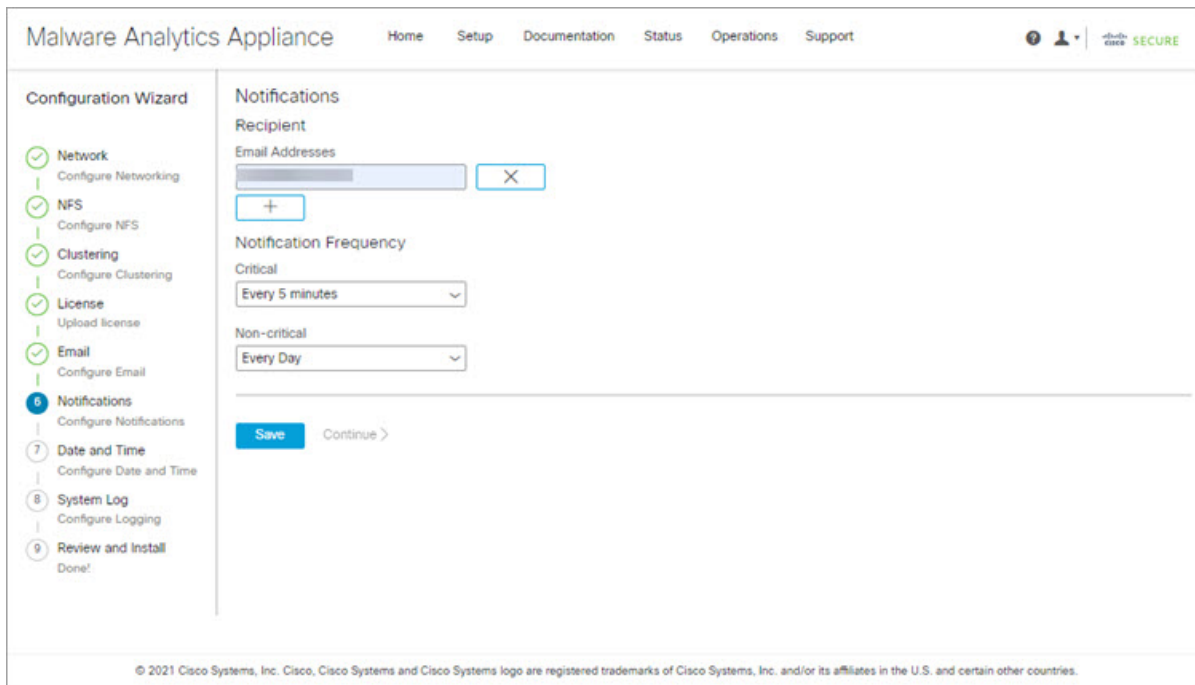
通知の設定

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 8: Notifications



The screenshot shows the Malware Analytics Appliance configuration wizard. The left sidebar lists the steps: Network, NFS, Clustering, License, Email, Notifications (current), 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 the 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.'

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 \(14 ページ\)](#) に進みます。

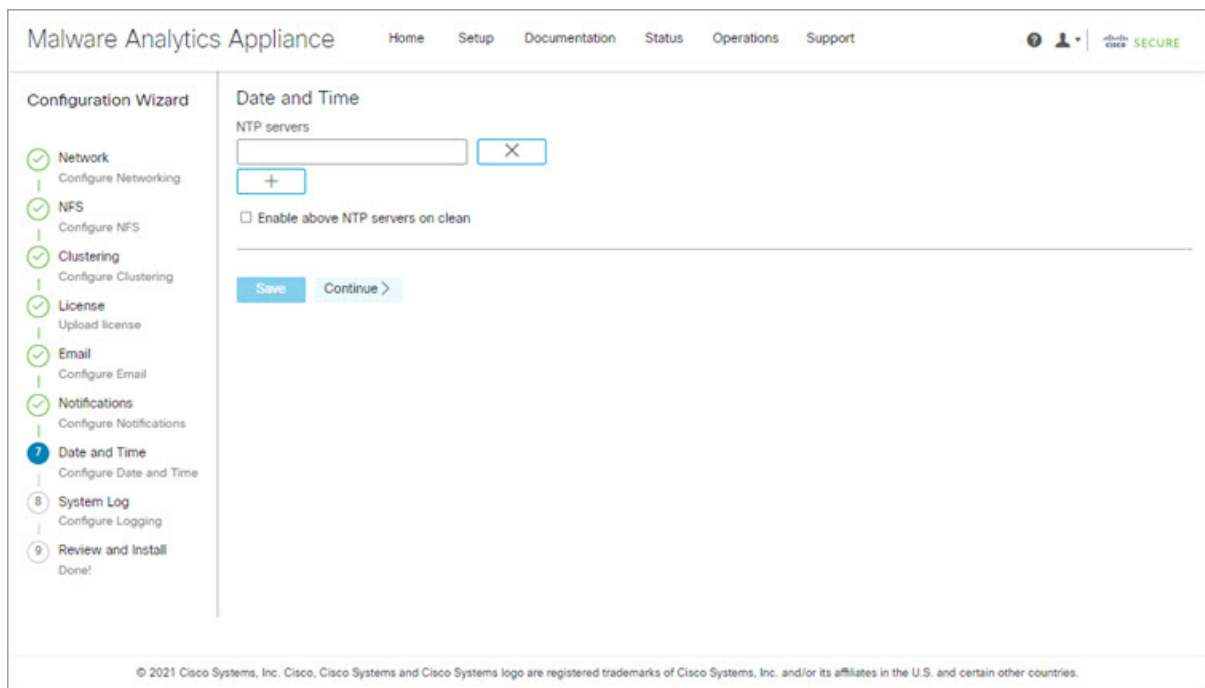
日付と時刻の設定

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 9: 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 \(15 ページ\)](#) に進みます。

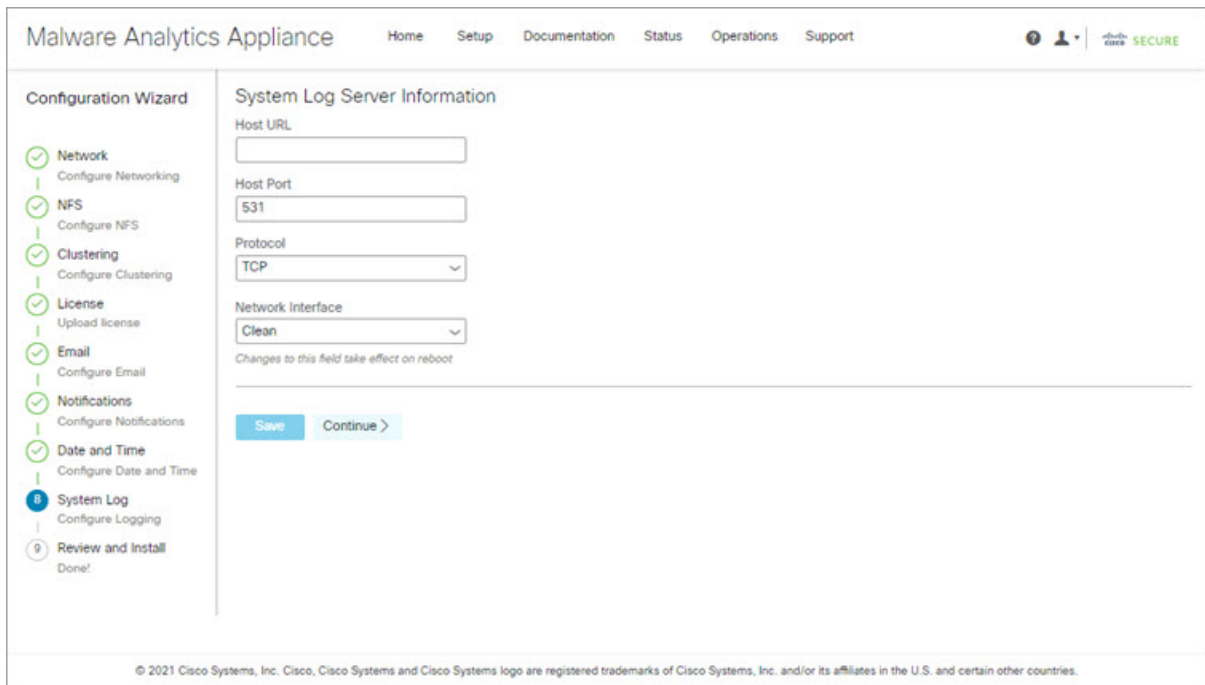
システムログの設定

[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 10: システムログサーバー情報



The screenshot shows the Malware Analytics Appliance configuration wizard. On the left is a 'Configuration Wizard' sidebar with steps: Network, NFS, Clustering, License, Email, Notifications, Date and Time, System Log (highlighted with a blue circle and '8'), and Review and Install. The main area is titled 'System Log Server Information' and contains fields for Host URL, Host Port (531), Protocol (TCP), and Network Interface (Clean). A 'Save' button and a 'Continue >' button are at the bottom. A copyright notice for Cisco Systems is at the very bottom.

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 \(15 ページ\)](#) に進みます。

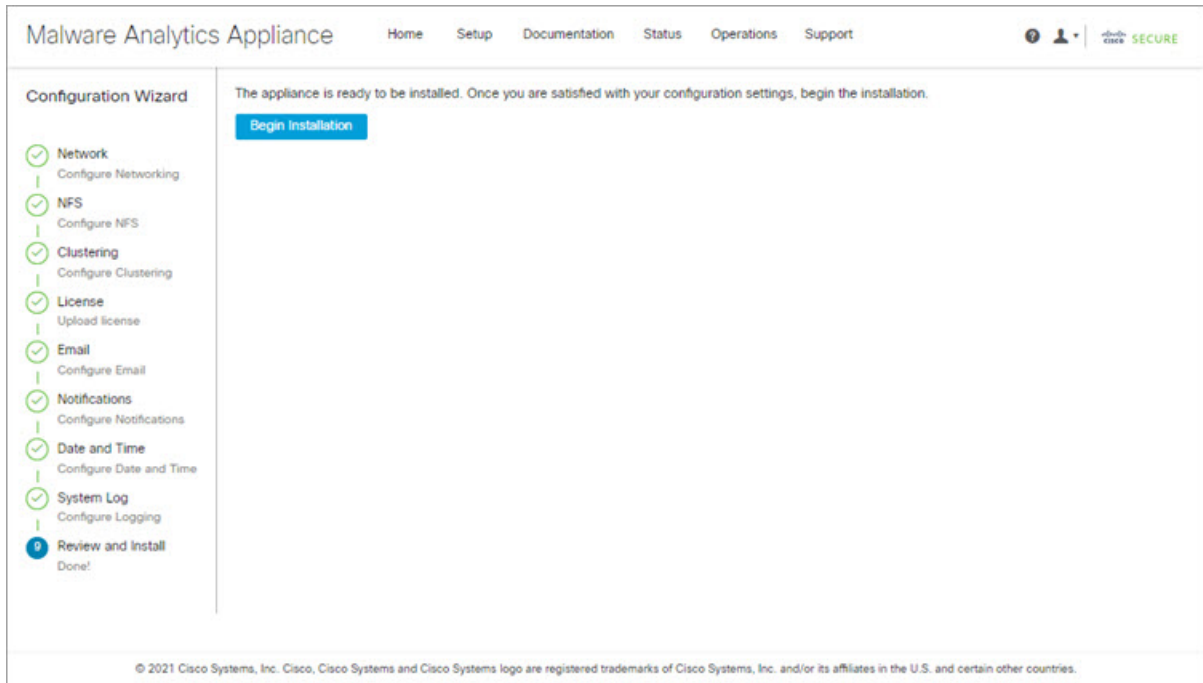
設定の確認とインストール

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。

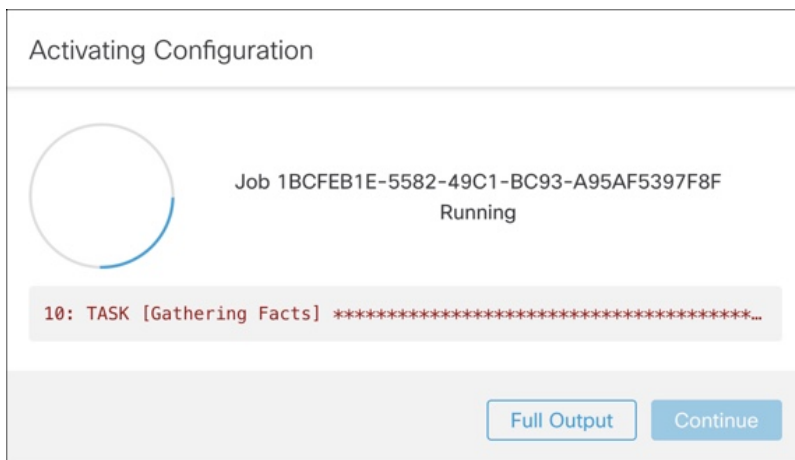
図 11: インストールの開始



(注)

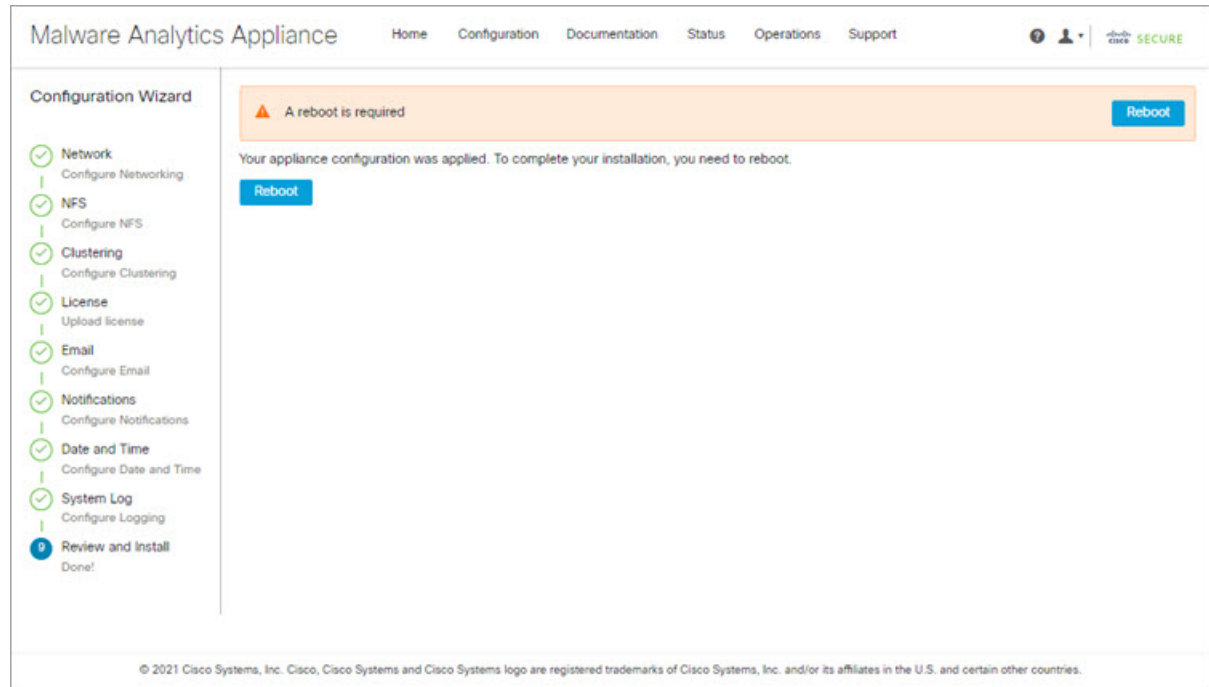
この画面には、設定の適用状況に応じて設定情報が表示されます。

図 12: 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 13: アプライアンスのインストール成功

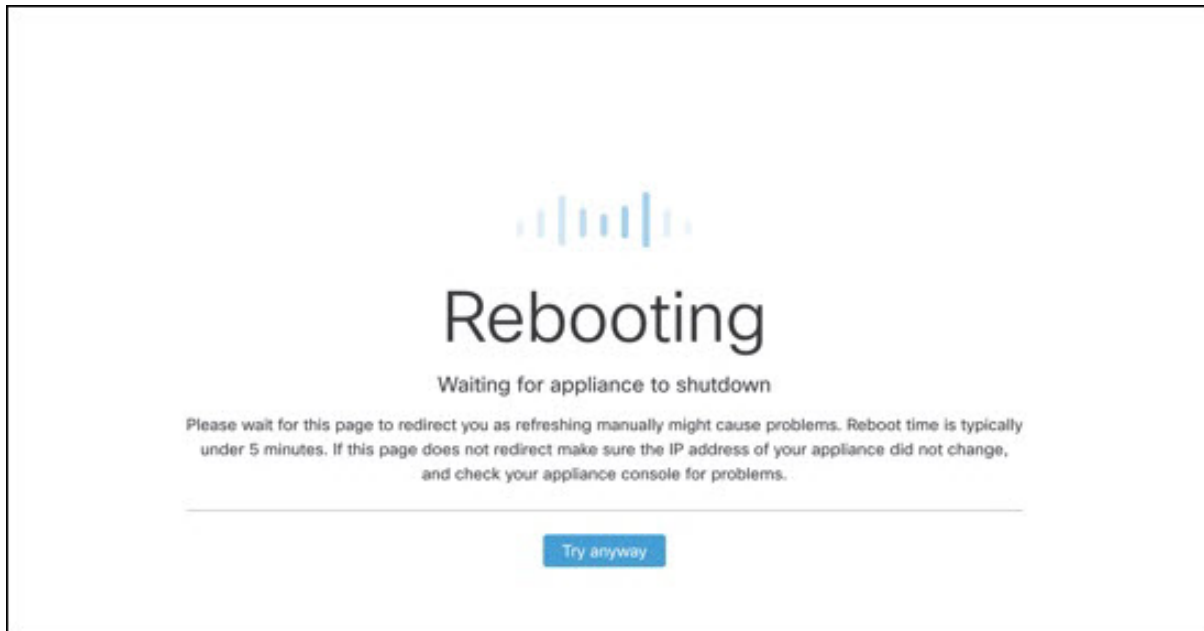


ステップ 2 [Reboot] をクリックします。

(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 14: 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、[Cisco Secure Malware Analytics アプライアンス 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。

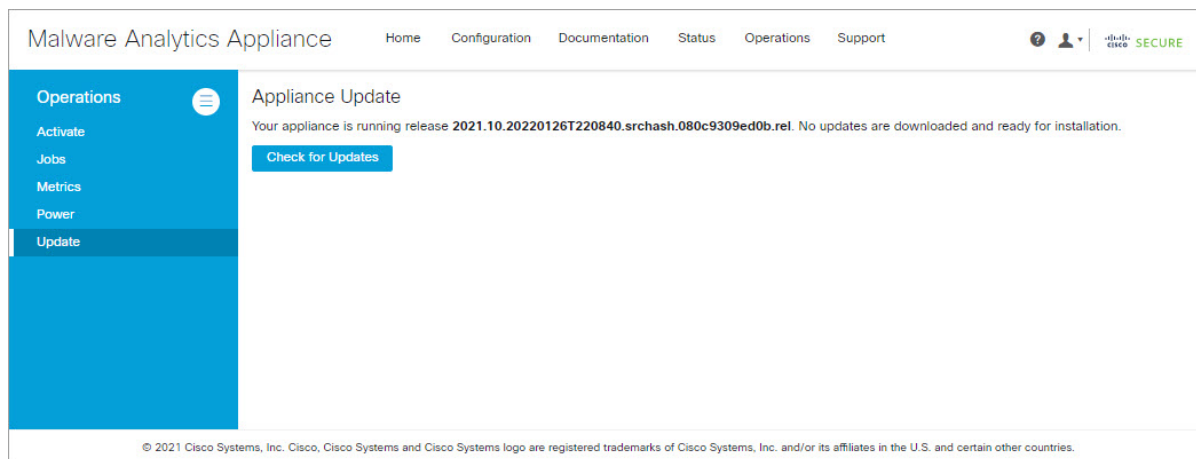


(注) 更新のインストールの詳細については、『[Cisco Secure Malware Analytics Appliance Administration Guide](#)』を参照してください。

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 15: 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

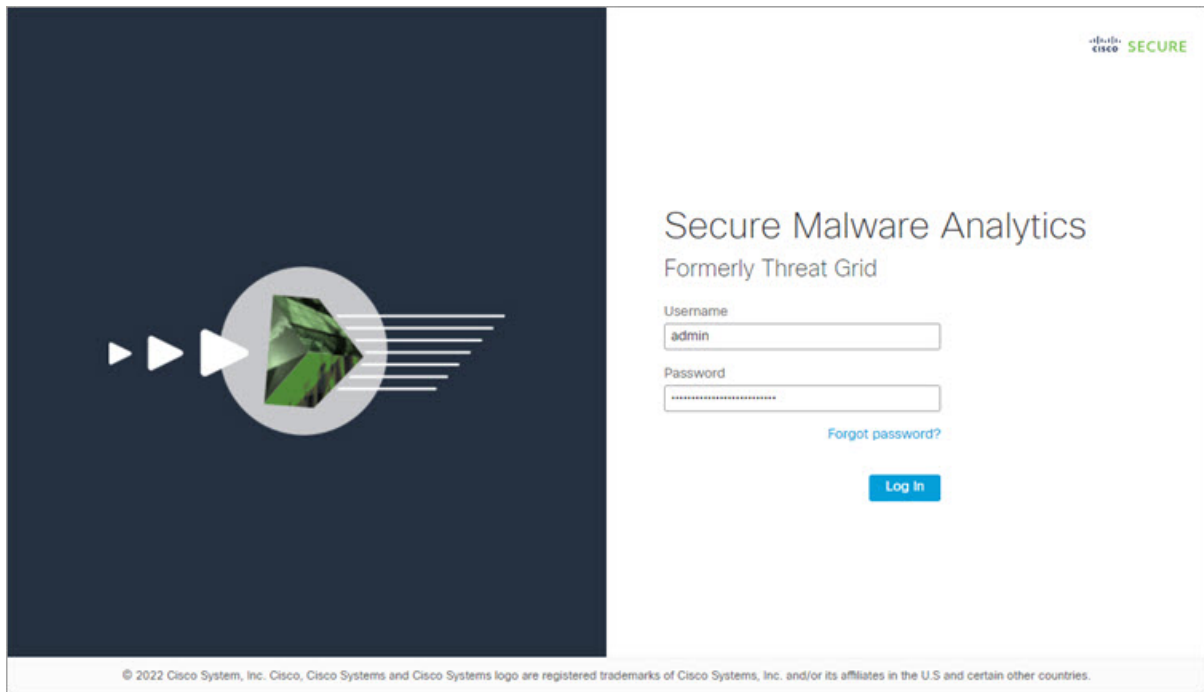
Cisco Secure Malware Analytics を使用アプライアンスが現行のバージョンに更新されたら、Cisco Secure Malware Analytics にマルウェアサンプルを送信して、アプライアンスが正しく設定されていることをテストする必要があります。

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 16: Cisco Secure Malware Analytics ログイン

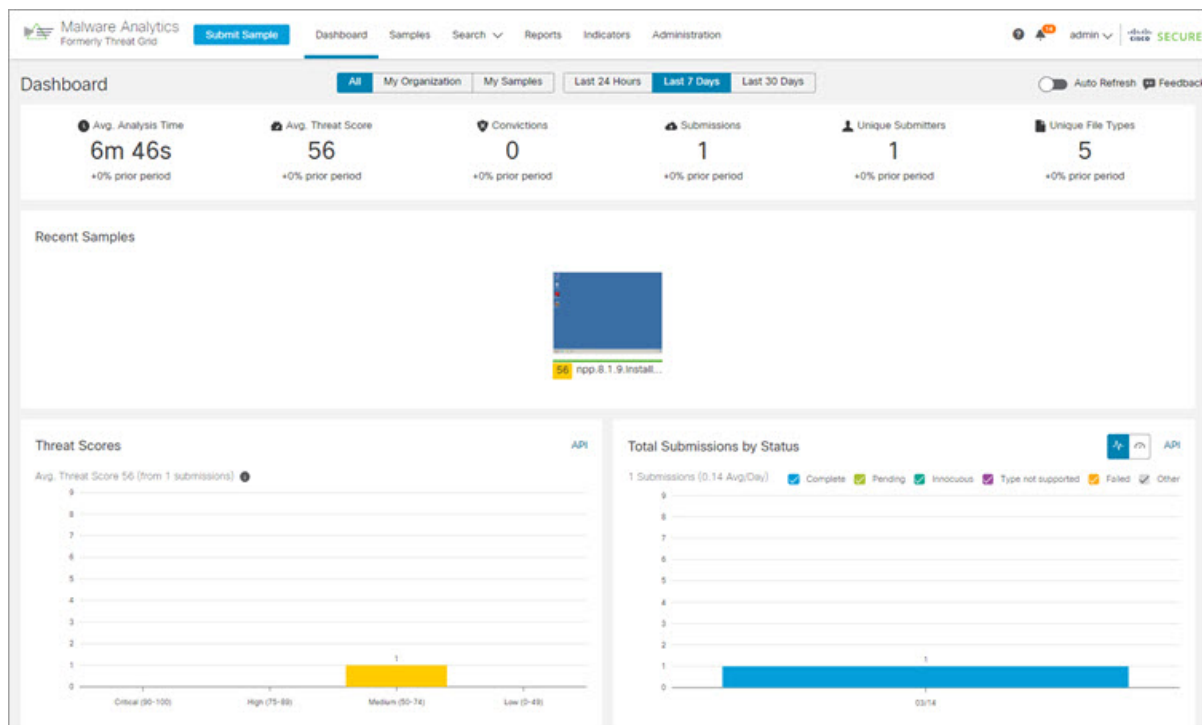


ステップ 2 次のデフォルトの資格情報を入力します。

- 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 17: 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 18: 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 19: 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 is divided into a left sidebar with navigation options like 'Metadata', 'Indicators', 'Network', etc., and a main content area. The main area is split 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	Q_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。