

セキュアなマルウェア分析サポートスナップショットの生成とライブサポートセッションの有効化

内容

[概要](#)

[スナップショットのサポート](#)

[管理UIからのサポートスナップショットの生成](#)

[TGSN CLIからのサポートスナップショットの生成](#)

[ライブサポートセッション](#)

[管理UIからのライブサポートセッションの有効化](#)

[TGSN CLIからのライブサポートセッションの有効化](#)

概要

このドキュメントでは、詳細な調査のために、Cisco Secure Malware Analytics アプライアンスからサポートスナップショットを収集し、ライブサポートセッションを有効にする手順について説明します

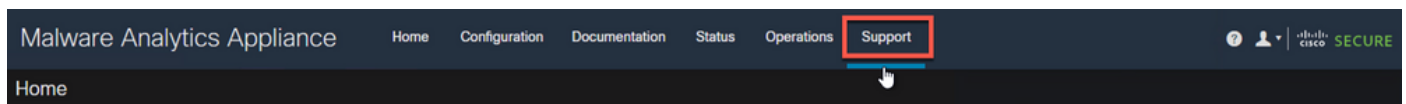
スナップショットのサポート

管理UIからのサポートスナップショットの生成

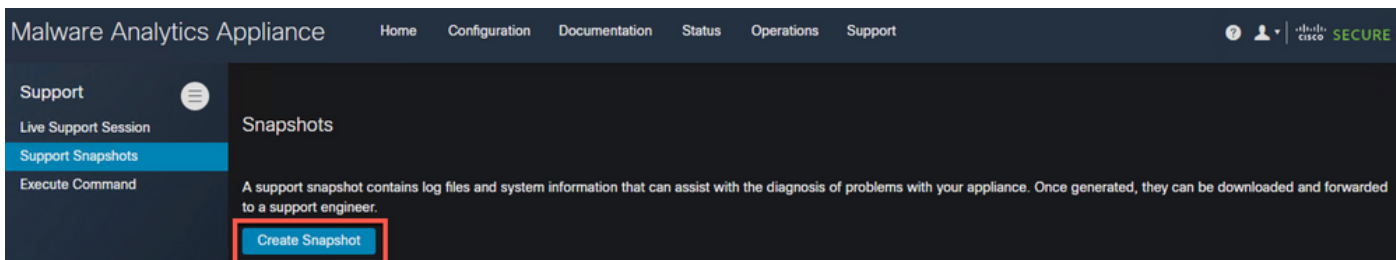
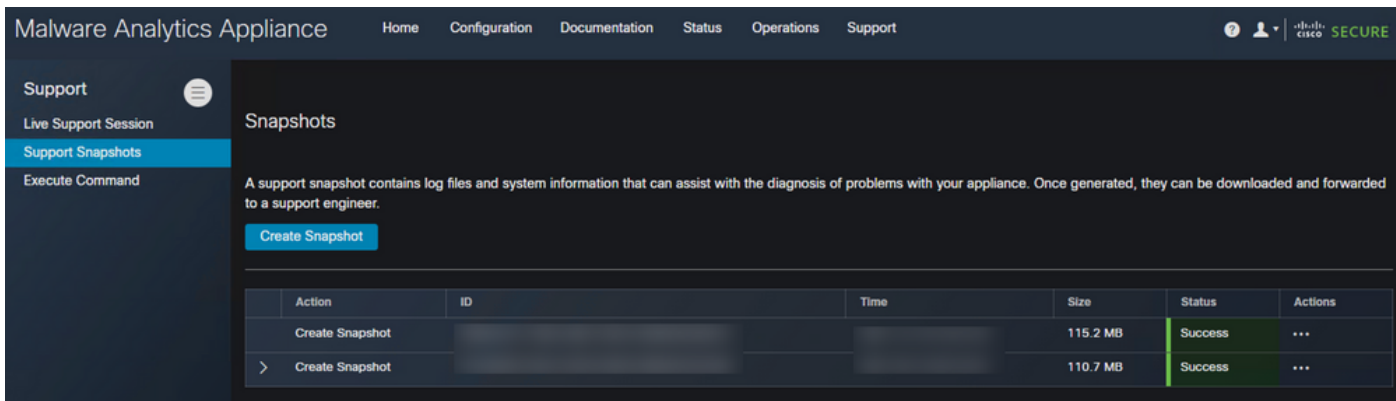
サポートスナップショットを作成するには、次の手順を実行します。

ステップ 1 : Secure Malware Analytics Admin UIにログインします

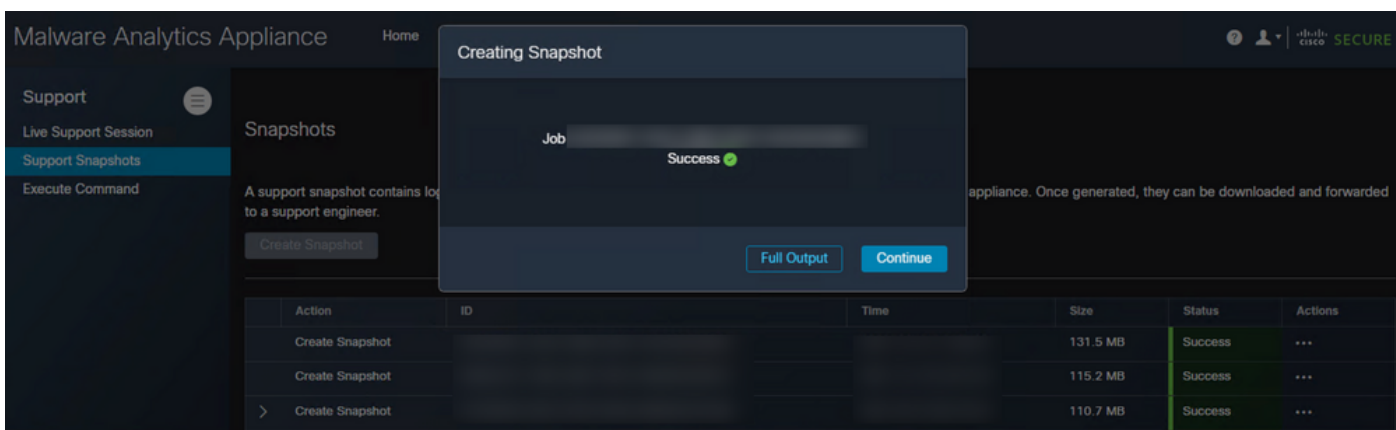
ステップ 2 : [サポート]をクリックまたは選択します



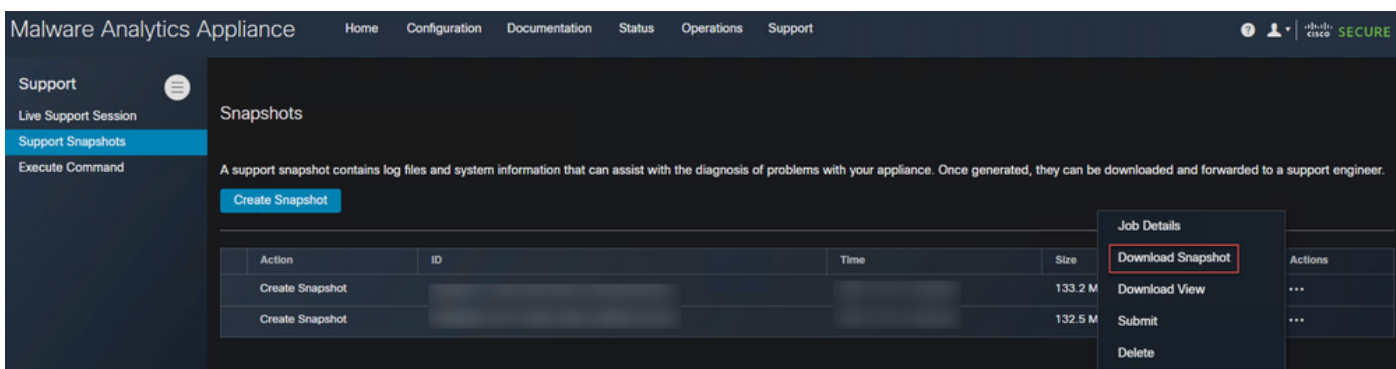
ステップ 3 : をクリックするか、[Support Snapshots]を選択し、をクリックするか、[Create Snapshot]を選択して、このアプライアンスでサポート・スナップショットを生成します



ステップ 4 : スナップショットが完了すると、次の図に示すように**Success**メッセージが表示されます。



ステップ 5 : [アクション]で[スナップショットのダウンロード]をクリックまたは選択します。これにより、UIにログインしたマシン上のスナップショットがダウンロードされます。



TGSH CLIからのサポートスナップショットの生成

TGSH CLIからサポートスナップショットを作成するには、次の手順を実行します。

ステップ 1 : SSHからTGSH CLIにログインします。このアクセスを設定する方法については、[ユ](#)

ーザガイドを参照してください

ステップ 2 : ログインしたら、[スナップショット]オプションを選択します

```
-----Cisco Secure Malware Analytics - Appliance Administration-----
Your Malware Analytics appliance can be managed at:
Admin URL / MAC:      https://
Application URL / MAC: https://
Password:             *** set by user ***

(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
```

ステップ 3 : [作成]オプションを選択すると、スナップショットが生成されます。これで、Admin UIで文書化されたプロセスに従って、Admin UIからスナップショットをダウンロードできます

```
-----Cisco Secure Malware Analytics - Appliance Administration-----
Your Malware Analytics appliance can be managed at:
Admin URL / MAC:      https://
Application URL / MAC: https://
Password:             *** set by user ***

-----Snapshots-----
Latest snapshot:

(c) Create
    Create Support Snapshot
(v) View
    View Support Snapshot
(s) Submit
    Submit Support Snapshot
(b) Back
    Back to main menu
```

ライブサポートセッション

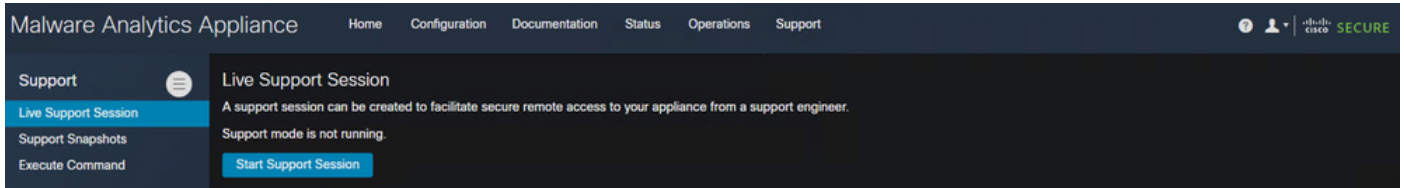
管理UIからのライブサポートセッションの有効化

ほとんどの場合、TACからSecure Malware Analyticsアプライアンスへのライブサポートセッションを有効にして、詳細な調査を依頼されることがあります

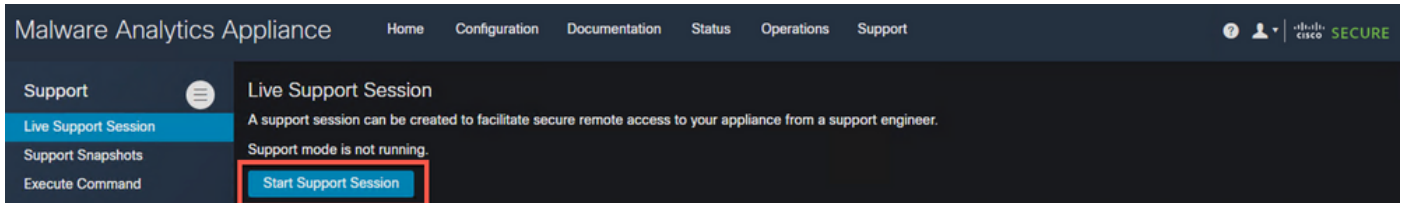
注 : TACへのライブサポートセッションを有効にするシリアル番号を入力して、デバイスへのリモートアクセスを有効にしてください

アプライアンスでこのアクセスを有効にするには、次の手順を実行します。

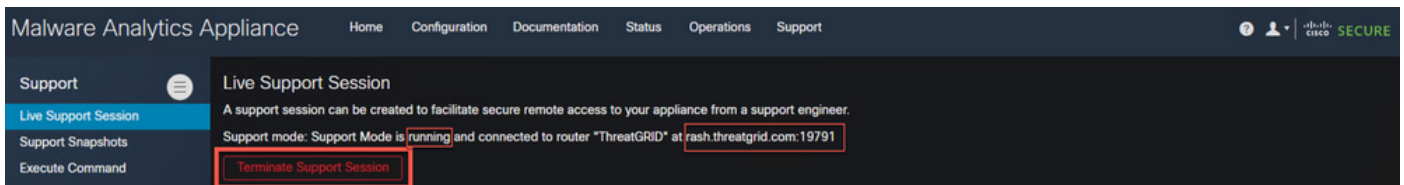
ステップ 1：管理UIで、[Support]タブの下の[Live Support Session]をクリックまたは選択してください



ステップ 2： をクリックするか、[サポートセッションの開始]オプションを選択します



ステップ 3：接続したら、次の図のようなメッセージが表示されます。



注：このアクセスが正しく動作するには、ダーティインターフェースから cure.threatgrid.com へのアウトバウンドコネクティビティを許可する必要があります。詳細は、「[ネットワーク・インターフェースの設定図](#)」を参照してください

TGSH CLIからのライブサポートセッションの有効化

SSHからTGSH CLIからアプライアンスでこのアクセスを有効にするには、次の手順を実行します。

ステップ 1：TGSH SSH CLIにログインします

ステップ 2：[サポートモード]オプションを選択します

```
-----Cisco Secure Malware Analytics - Appliance Administration-----
Your Malware Analytics appliance can be managed at:
Admin URL / MAC:      https://
Application URL / MAC: https://
Password:             *** set by user ***

(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
```

ステップ 3 : [開始]を選択して、ライブセッションを有効にします

```
-----Cisco Secure Malware Analytics - Appliance Administration-----
Your Malware Analytics appliance can be managed at:
Admin URL / MAC:      https://
Application URL / MAC: https://
Password:             *** set by user ***

Support Mode-----
Status: inactive

(s) Start
    Start support mode
(b) Back
    Back to main menu
```

ステップ 4 : ステータスがアクティブと表示されていることを確認する必要があります

```
-----Cisco Secure Malware Analytics - Appliance Administration-----
Your Malware Analytics appliance can be managed at:
Admin URL / MAC:      https://
Application URL / MAC: https://
Password:             *** set by user ***

Support Mode-----
Status: active

(t) Stop
    Stop support mode
(b) Back
    Back to main menu
```

注 : 管理UIまたはTGSN CLIアクセスが使用できない場合は、アプライアンスの回復モードからライブサポートセッションを有効にすることもできます。