

# Gerar instantâneo de suporte do Secure Malware Analytics e ativar a sessão de suporte ao vivo

## Contents

[Introduction](#)

[Snapshots de suporte](#)

[Gerar instantâneo de suporte da IU do administrador](#)

[Gerar instantâneo de suporte da CLI TGSH](#)

[Sessão de suporte ao vivo](#)

[Habilitar sessão de suporte ao vivo da IU do administrador](#)

[Habilitar sessão de suporte ao vivo do TGSH CLI](#)

## Introduction

Este documento descreve as informações sobre as etapas para coletar o instantâneo de suporte e ativar a sessão de suporte ao vivo do dispositivo Cisco Secure Malware Analytics para uma investigação mais detalhada

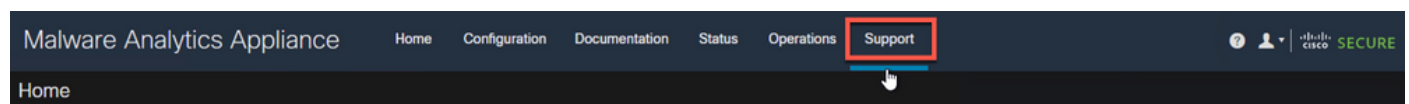
## Snapshots de suporte

### Gerar instantâneo de suporte da IU do administrador

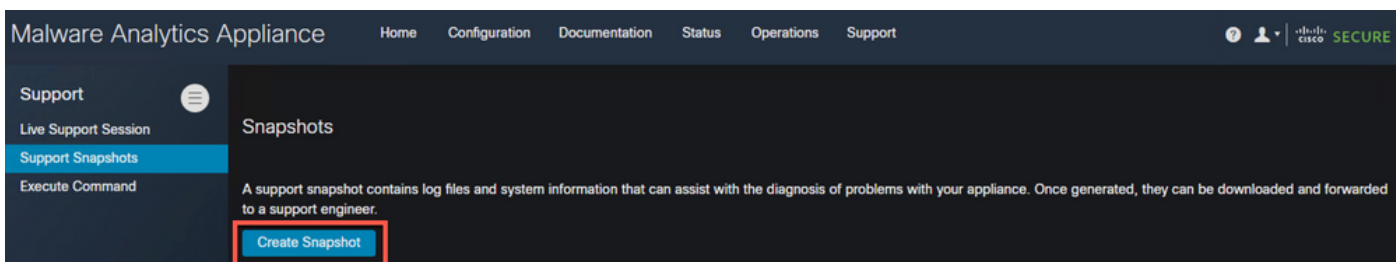
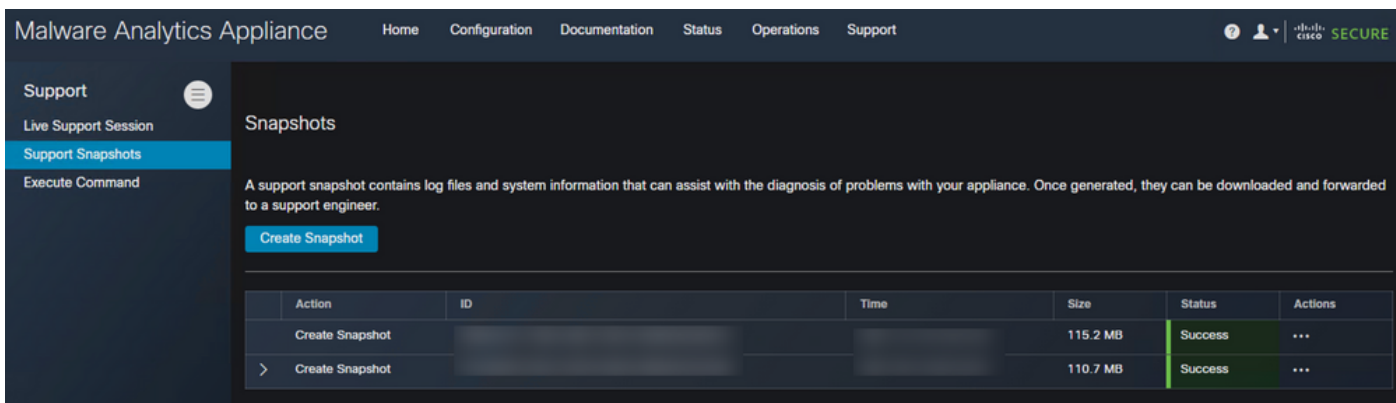
Para criar um Snapshot de suporte, siga estas etapas:

Passo 1: Faça login na interface de usuário do administrador do Secure Malware Analytics

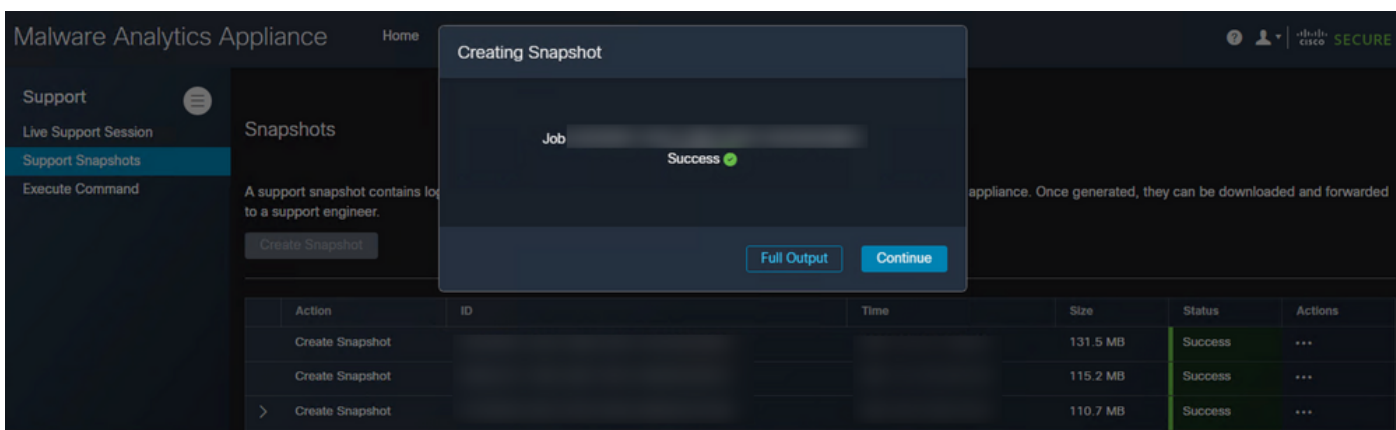
Passo 2: clique em ou selecione **Suporte**



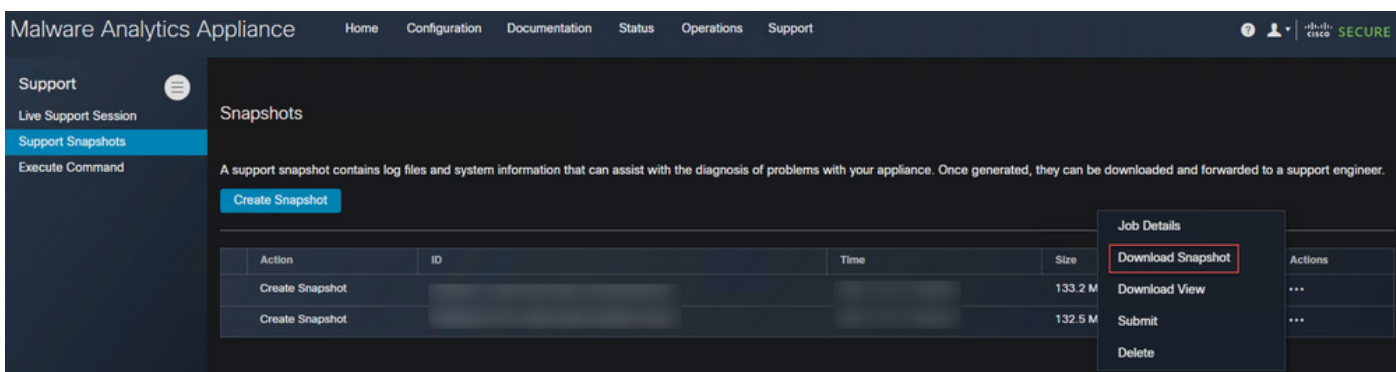
Passo 3: clique em ou selecione **Support Snapshots** e clique em ou selecione **Create Snapshot** para gerar um snapshot de suporte neste aplicativo



Passo 4: Quando o snapshot estiver concluído, você verá uma mensagem **Success** como mostrado na imagem:



Passo 5: Em **Ações**, clique ou selecione **Baixar instantâneo** e isso deve fazer o download do instantâneo na sua máquina de onde você fez login na interface do usuário



## Gerar instantâneo de suporte da CLI TGSH

Para criar um Snapshot de suporte da CLI TGSH, siga estas etapas:

Passo 1: Faça login na CLI TGSH do SSH. Consulte o [Guia do usuário](#) para obter instruções

sobre como configurar esse acesso

Passo 2: Quando estiver conectado, selecione a opção **Snapshots**

```
-----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
```

Passo 3: Selecione a opção **Create** e isso gera o Snapshot. Agora, você poderá fazer o download do Snapshot da IU do administrador de acordo com o processo documentado para a IU do administrador

```
-----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
```

## Sessão de suporte ao vivo

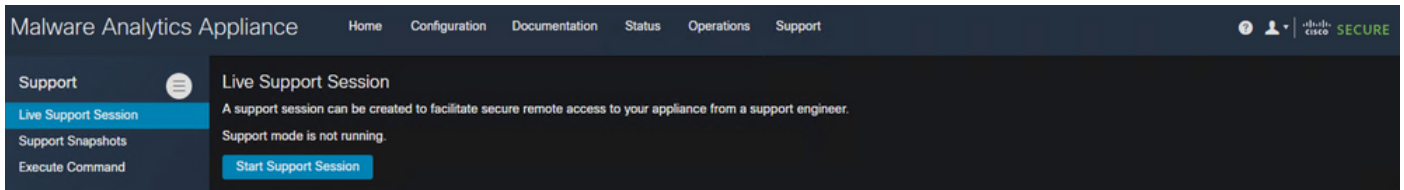
### Habilitar sessão de suporte ao vivo da IU do administrador

Na maioria dos casos, o TAC pode solicitar que você habilite a sessão de suporte ao vivo para o aplicativo Secure Malware Analytics para uma investigação mais detalhada

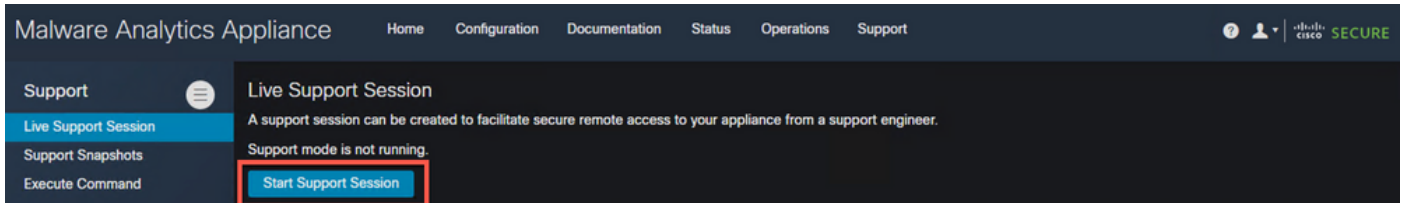
NOTE: Forneça o número de série que você habilita a sessão de suporte ao vivo no TAC para permitir que eles acessem o dispositivo remotamente

Para habilitar esse acesso no dispositivo, siga estas etapas:

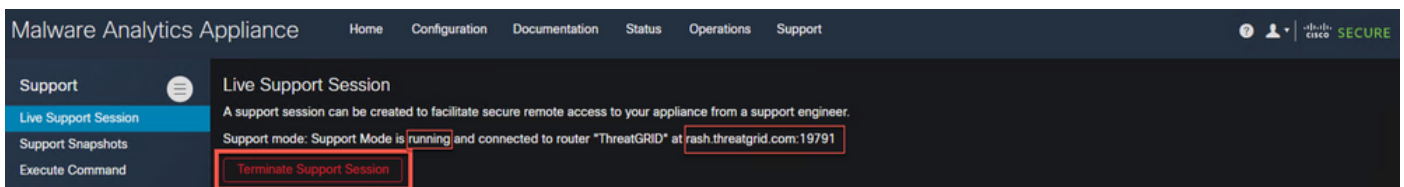
Passo 1: Na IU do administrador, clique ou selecione a **Sessão de suporte ao vivo** na guia **Suporte**



Passo 2: clique ou selecione a opção **Iniciar sessão de suporte**



Passo 3: Depois de conectado, você deve ver a mensagem como mostrado na imagem:



Note: Você precisa permitir que a conectividade de saída da interface **suja** para **rash.ameaçgrid.com** para que esse acesso funcione corretamente. Consulte o [Diagrama de Configuração da Interface de Rede](#) para obter mais informações

## Habilitar sessão de suporte ao vivo do TGSH CLI

Para habilitar esse acesso no dispositivo da CLI TGSH do SSH, siga estas etapas:

Passo 1: Faça login na CLI SSH do TGSH

Passo 2: Selecione a opção **Support Mode (Modo de suporte)**

```
-----Cisco Secure Malware Analytics - Appliance Administration-----
Your Malware Analytics appliance can be managed at:
Admin URL / MAC:      https://[REDACTED]
Application URL / MAC: https://[REDACTED]
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
```

Passo 3: Selecione **Start** para habilitar a sessão Live

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

Support Mode-----
Status: inactive

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

Passo 4: Você deve vê-lo mostrando o Status como **ativo**

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

Support Mode-----
Status: active

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

Note: Em situações em que o acesso à interface do usuário do administrador ou à CLI do TGSN não está disponível, a sessão de suporte ao vivo também pode ser ativada no modo de recuperação do aplicativo.