

Genere una instantánea de soporte de Secure Malware Analytics y habilite la sesión de soporte en directo

Contenido

[Introducción](#)

[Admitir instantáneas](#)

[Generar instantánea de soporte desde la IU de administrador](#)

[Generar instantánea de compatibilidad desde TGSN CLI](#)

[Sesión de asistencia en directo](#)

[Activar sesión de Live Support desde la IU de administrador](#)

[Activar sesión de asistencia en directo desde TGSN CLI](#)

Introducción

Este documento describe la información sobre los pasos para recopilar la instantánea de soporte y habilitar la sesión de soporte en vivo desde el dispositivo Cisco Secure Malware Analytics para una investigación adicional

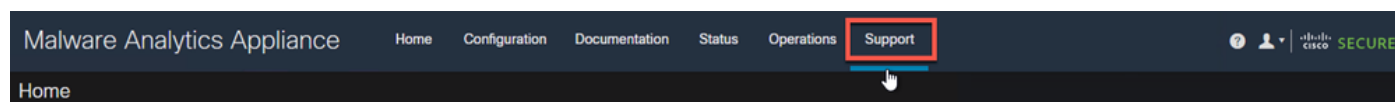
Admitir instantáneas

Generar instantánea de soporte desde la IU de administrador

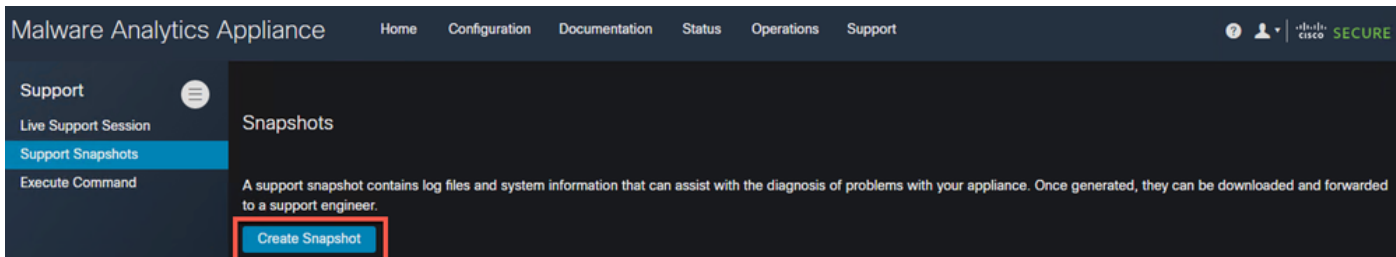
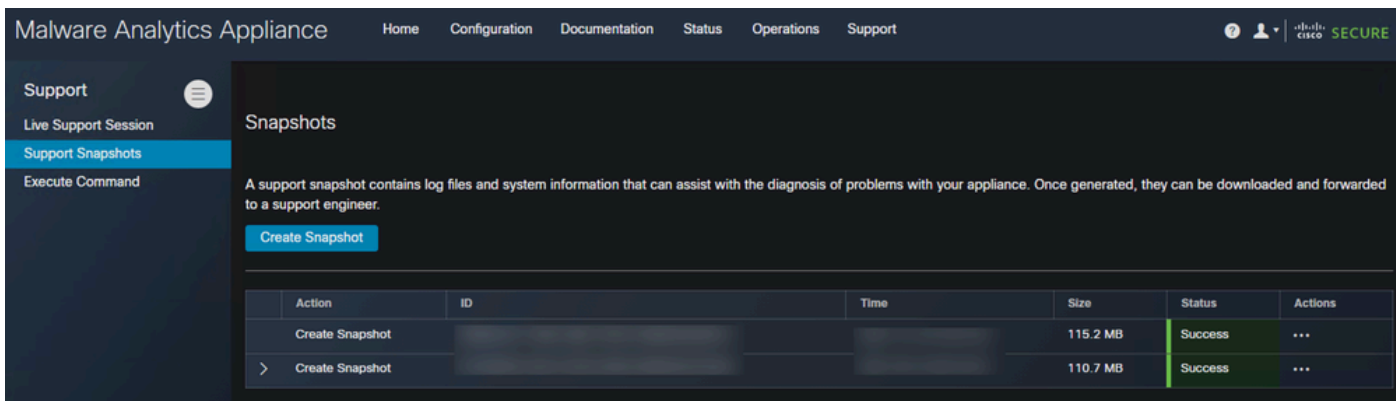
Para crear una instantánea de soporte, siga estos pasos:

Paso 1: Inicie sesión en la IU de administración de Secure Malware Analytics

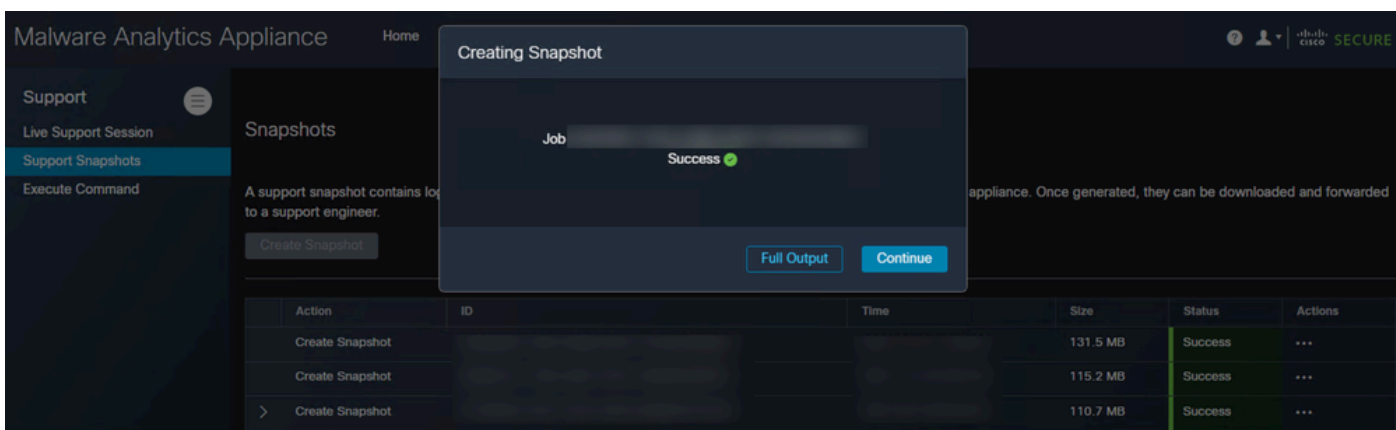
Paso 2: haga clic o seleccione Support (Asistencia)



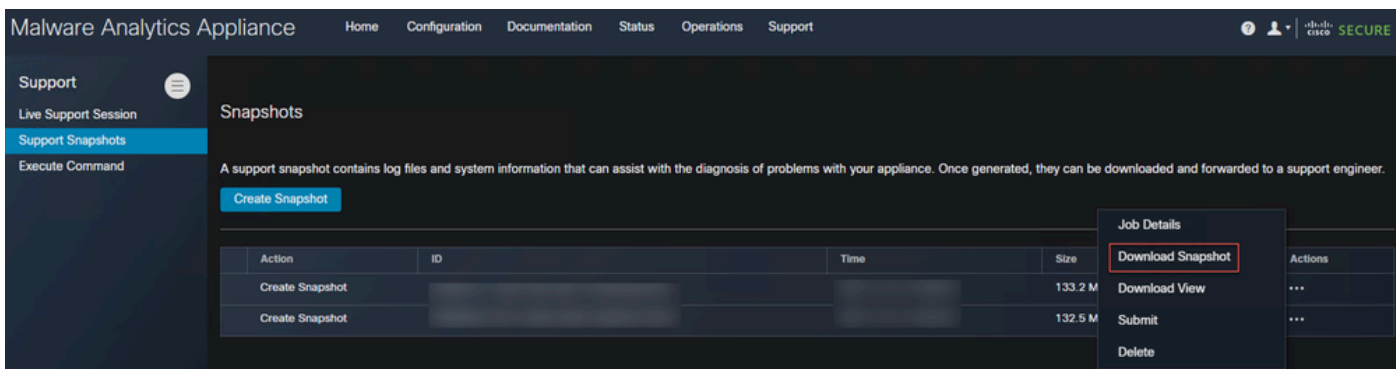
Paso 3: haga clic en Support Snapshots o selecciónelo y, a continuación, haga clic en Create Snapshot para generar una instantánea de soporte en este dispositivo



Paso 4: Una vez que se complete la instantánea, verá un mensaje de éxito como se muestra en la imagen:



Paso 5: en Acciones, haga clic en o seleccione Descargar instantánea y debe descargar la instantánea en su equipo desde donde inició sesión en la interfaz de usuario



Generar instantánea de compatibilidad desde TGS CLI

Para crear una instantánea de soporte desde TGS CLI, siga estos pasos:

Paso 1: Inicie sesión en TGSN CLI desde SSH. Consulte la [guía del usuario](#) para obtener instrucciones sobre cómo configurar este acceso

Paso 2: Una vez que haya iniciado sesión, seleccione la opción Instantáneas

```
-----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
```

Paso 3: Seleccione la opción Create y se generará la instantánea. Ahora, podrá descargar la instantánea desde la interfaz de usuario del administrador según el proceso documentado para la interfaz de usuario del administrador

```
-----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 ***

-----Snapshots-----
Latest snapshot: [redacted]

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

Sesión de asistencia en directo

Activar sesión de Live Support desde la IU de administrador

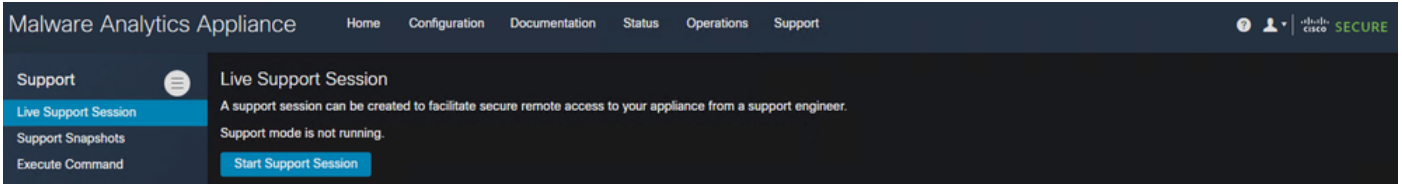
En la mayoría de los casos, el TAC puede solicitarle que active la sesión de asistencia en directo en el dispositivo Secure Malware Analytics para realizar investigaciones adicionales

NOTA: Indique el número de serie con el que activa la sesión de asistencia en directo al TAC para

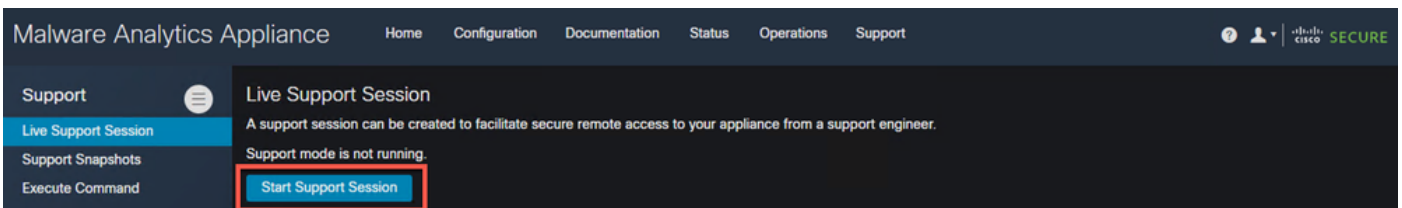
que pueda acceder al dispositivo de forma remota

Para activar este acceso en el dispositivo, siga estos pasos:

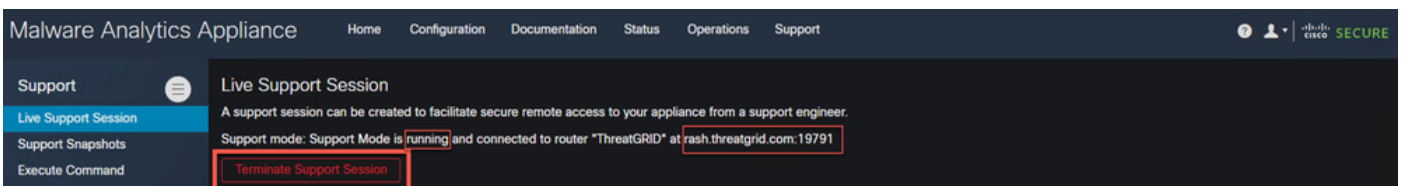
Paso 1: En la interfaz de usuario de administración, haga clic en o seleccione la Sesión de soporte en directo en la pestaña Soporte.



Paso 2: haga clic en o seleccione la opción Iniciar sesión de soporte



Paso 3: Una vez conectado, debe ver el mensaje como se muestra en la imagen:



Nota: Debe permitir la conectividad saliente desde la interfaz Dirty a rash.threatGrid.com para que este acceso funcione correctamente. Consulte el [Diagrama de Configuración de la Interfaz de Red](#) para obtener más información

Activar sesión de asistencia en directo desde TGSH CLI

Para habilitar este acceso en el dispositivo desde TGSH CLI desde SSH, siga estos pasos:

Paso 1: Inicie sesión en TGSH SSH CLI

Paso 2: Seleccione la opción Support Mode

```
-----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
```

Paso 3: Seleccione Start para habilitar la sesión en directo

```
-----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
```

Paso 4: Debe verlo mostrando el estado como activo

```
-----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
```

Nota: en situaciones en las que el acceso a la interfaz de usuario de administración o a la CLI de

TGSH no esté disponible, la sesión de Live Support también se puede habilitar desde el modo de recuperación del dispositivo.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).